LIVRES VERTS CA

Gestion des réseaux et de la voix

SOLUTION INTÉGRÉE DE GESTION DES DÉFAILLANCES ET DES PERFORMANCES

- Présentation de l'évolution des réseaux convergents et des besoins de gestion
- Recommandations relatives au déploiement de la solution de gestion des réseaux et de la voix de CA



AVERTISSEMENT LÉGAL



REMERCIEMENTS

CA remercie les personnes suivantes pour leur contribution à ce livre vert :

Auteurs principaux

Don LeClair
Sue Andersen
Jason Bryk
Roger Craig
Bill Donoghue
Justin Gagnon
Brian Gollaher
Andrew Haigh
Kathleen Hickey
Mark Hounslow
John Kane
Michael Marks
John Murdough
Barbara O'Toole
Pete Oliveira
Jason Warfield
Dianne Weiss

Les auteurs principaux et CA tiennent à remercier les collaborateurs suivants :

Ajei Gopal
Tricia Bancroft
Lynn Beck
Gregory Buonaiuto
Curtis Lehman
Peter Clairmont
Dan Lewis
Anders Magnusson
Alexandre Moscoso
Joe Pennachio
David Soares
Peter Skotny
Cheryl Stauffer
Tom Wilson



RÉFÉRENCES AUX PRODUITS CA

- Gestion des réseaux et de la voix de CA
- *e*Health®
- *e*Health® for Voice
- SPECTRUM®
- *e*Health® for Voice Policy Manager
- *e*Health® E2E Console
- *e*Health® Live Health
- *e*Health® Traffic Accountant
- *e*Health® Universal Workflow Integration Modules
- *e*Health® Universal Data Integration Modules
- *e*Health® Universal Wireless Integration Modules
- SPECTRUM® Infinity
- SPECTRUM® Integrity
- SPECTRUM® Xsight
- SPECTRUM® OneClick
- SPECTRUM® Service Manager
- SPECTRUM® Report Manager
- SPECTRUM® Alarm Notification Manager
- SPECTRUM® ATM Circuit Manager
- SPECTRUM® Configuration Manager
- SPECTRUM® Secure Domain Manager
- SPECTRUM® Frame Relay Manager
- SPECTRUM® Microsoft Operations Manager Connector
- SPECTRUM® Multicast Manager
- SPECTRUM® OSS Integrations
- SPECTRUM® QoS Manager
- SPECTRUM® Remedy ARS Gateway
- SPECTRUM® SNMPv3 Support
- SPECTRUM® VPN Manager
- SPECTRUM® Watch Editor
- SPECTRUM® Service Performance Manager
- SPECTRUM® Assurance Server Xsight
- SPECTRUM® Assurance Server Integrity
- SPECTRUM® Assurance Server Infinity



Sommaire









Chapitre 1 : Introduction

A propos de ce livre

Le livre vert CA sur la gestion des réseaux et de la voix explique comment gérer les performances et la disponibilité des réseaux convergents. La solution CA permet une gestion proactive des services de voix et de données, garantit une bande passante et une capacité système suffisantes et prend en charge les niveaux de service orientés métier. Avec des fonctions intégrées d'administration des performances et des erreurs réseau, elle offre la possibilité d'exploiter le réseau en tant que plate-forme de fourniture de service.

Le présent livre vert CA s'adresse aux opérateurs réseau, aux ingénieurs et aux techniciens chargés de la gestion des réseaux de voix et de données. Les exemples de déploiement illustrés présentent les différents aspects d'une petite entreprise et d'un grand fournisseur de services. Ces informations peuvent se révéler utiles pour de nombreux autres déploiements réseau, mais peuvent aussi varier en fonction des exigences réseau.

Ce livre vert CA présente les fonctionnalités qui permettent aujourd'hui de gérer un réseau convergent. Les premières sections offrent un aperçu stratégique des tendances vers les réseaux convergents. Les sections suivantes présentent les recommandations de déploiement et d'utilisation de la solution CA de gestion des réseaux et de la voix à des fins de gestion d'un réseau convergent.

Ce livre vert CA contient uniquement des informations sur la gestion des réseaux et de la voix. Il appartient à une série de livres verts CA conçus pour définir les fonctionnalités des principales solutions CA et présenter les recommandations relatives à la gestion et à la sécurisation de ces solutions. D'autres livres verts CA décrivent les solutions utilisées pour diverses tâches de gestion informatique telles que la gestion des systèmes ou des bases de données et l'automatisation de la charge de travail.

Ce livre vert sur la gestion des réseaux et de la voix est destiné aux responsables informatiques, aux équipes de gestion réseau et au personnel technique. Il est organisé comme suit :

- **Les chapitres 1 à 3**, destinés aux responsables informatiques et aux gestionnaires réseau, présentent les défis à relever en matière de gestion des réseaux convergents, ainsi que les avantages de la solution de gestion des réseaux et de la voix de CA.
- **Les chapitres 4 à 10** s'adressent aux gestionnaires réseau et au personnel technique. Ils présentent des exemples de déploiement de produits intégrant la solution de gestion des réseaux et de la voix de CA. Ces chapitres présentent également les recommandations en matière de planification, de déploiement et de configuration de la solution afin d'accélérer le retour sur l'investissement consacré à l'optimisation du réseau.

Ce livre vert CA aborde également les sujets suivants :

- Descriptions techniques des composants de la solution recommandée.
- Recommandations en matière d'installation et de configuration des composants de la solution.
- Définition et gestion des niveaux de service réseau.
- Recommandations en matière d'activation de l'assurance proactive des services et de résolution rapide des problèmes.
- Exécution de la planification de la capacité et gestion des réseaux de voix et de données.



Présentation

Evolution des exigences en termes de gestion des réseaux et de la voix

Toute l'infrastructure informatique dépend du réseau. Récemment, l'utilisation du réseau a considérablement changé : les applications de voix et de données ainsi que les solutions vitales ont convergé, la diffusion de contenu vidéo venant également s'y ajouter. Les défaillances et les problèmes de performances du réseau ont des conséquences négatives immédiates pour l'entreprise en termes de productivité, de coûts et de revenus.

Ainsi, l'intérêt pour les erreurs et problèmes de performances du réseau, ainsi que la connaissance de ces erreurs et problèmes, concernent désormais un public plus étendu d'utilisateurs professionnels non experts qui recherchent des informations en temps réel, seules susceptibles de répondre à leurs besoins. En outre, l'équipe chargée d'exploiter les réseaux doit rapidement se familiariser avec de nouvelles technologies et étendre ses responsabilités en matière de gestion à la prise en charge des réseaux de voix et de données convergents.

Dans cet environnement, les solutions de gestion réseau doivent fournir des informations vitales et des fonctionnalités de gestion adaptées aux techniciens comme aux non-techniciens. Outre la gestion standard des défaillances et des performances, elles doivent proposer des alertes configurables, des tableaux de bord et des fonctionnalités analytiques à tous les utilisateurs.

Les solutions actuelles de gestion de réseaux et de voix doivent prendre en charge les éléments suivants :

- **Réseaux hétérogènes.** Elles doivent prendre en charge les technologies de données telles que le protocole Internet (IP), le mode de transfert asynchrone (ATM), le relais de trames (FR) et la transmission à large bande, ainsi que les infrastructures de voix intégrant le multiplexage sur répartition dans le temps (MRT), la téléphonie sur IP analogique et des infrastructures hybrides.
- **Echelle.** Elles doivent prendre en charge de vastes réseaux répartis sur plusieurs pays et continents et accepter des équipes de gestion réseau centrales ou régionales.
- **Intégration**. Elles doivent permettre l'utilisation d'une solution unique pour gérer les infrastructures de données et de voix et les systèmes vitaux.
- **Informations sur les services à partir des rôles.** Elles doivent prendre en charge la communication avec des clients externes à l'aide de contrats de niveau de service (SLA, Service Level Agreement) et avec des clients internes à l'aide de contrats de niveau d'exploitation (OLA, Operational Level Agreement) ou de mécanismes moins formels. Elles doivent permettre aux techniciens et aux utilisateurs orientés métier d'évaluer la capacité du réseau à soutenir l'activité, ainsi qu'à identifier et localiser la cause première des problèmes.



Solution de gestion des réseaux et de la voix de CA

La solution de gestion des réseaux et de la voix de CA assure la gestion convergente des données et de la voix. Elle permet aux services informatiques de gérer intégralement les services de voix et de données de manière proactive, d'assurer une capacité suffisante pour la bande passante et les systèmes et de prendre en charge les niveaux de service définis par l'entreprise. Cette solution est un élément clé de l'approche Enterprise IT Management (EITM), qui est la démarche de CA consistant à gérer et à sécuriser les environnements informatiques de manière dynamique, pour aider les entreprises à exploiter tout le potentiel de leur infrastructure informatique.

La solution de gestion des réseaux et de la voix de CA englobe les technologies IP et de voix existantes, ce qui permet aux entreprises de passer à la téléphonie IP à leur rythme et de réduire la complexité inhérente à la gestion d'infrastructures hétérogènes.

Cette solution intégrée et éprouvée offre les avantages suivants :

- **Gestion efficace des niveaux de service.** Définit des lignes de référence, évalue et assure le suivi des services du réseau. Diffuse des informations sur le respect des contrats de niveaux de service et d'exploitation auprès des utilisateurs orientés métier et des technicians.
- **Assurance proactive des services.** Les fonctions de surveillance, définies par des stratégies, servent à identifier les dégradations de services avant qu'elles ne se répercutent sur les clients et les utilisateurs finals.
- **Détection rapide des problèmes.** Elimine la véritable cause du problème grâce aux fonctions de corrélation des événements, d'analyse de la cause première (RCA) et de liaison avec la génération de rapports historiques et en temps réel.
- **Planification prédictive de la capacité.** Les algorithmes intelligents intégrés permettent aux équipes chargées de l'exploitation réseau d'identifier la date et l'emplacement des changements de circuits et de matériel à effectuer afin de maintenir le service dans les plages de performance attendues.

La solution de gestion des réseaux et de la voix de CA comporte trois composants principaux, chacun offrant un ensemble cohérent de fonctionnalités valables dans toute l'infrastructure de voix et de données.

- ***e*Health Network Performance Management :** recueille et stocke les données de performances vitales de plus de 100 fournisseurs et 1 000 périphériques ; applique des algorithmes intelligents aux données de performances afin d'identifier la dégradation de service, les soucis de planification de la capacité et la cause des problèmes de performances.
- **SPECTRUM Fault Management :** permet la gestion des défaillances, l'analyse de la cause première et la gestion des niveaux de service.
- ***e*Health for Voice :** permet la gestion des défaillances et des performances des systèmes de communication IP et MRT, des systèmes de messagerie et des autocommutateurs privés.



Cette solution puissante et unique permet de gérer des services réseau de plus en plus complexes dans les environnements d'entreprise, gouvernementaux et de télécommunications. Elle permet aux équipes techniques d'améliorer la qualité de leurs services, de maîtriser les coûts, de réduire les risques, d'augmenter les revenus et d'accroître leur efficacité lorsqu'elles gèrent l'infrastructure informatique comme un service métier.

Pour garantir la réussite des implémentations, l'organisation CA Technology Services™ aide toute entreprise à évaluer, concevoir, implémenter et optimiser les solutions de performance et de disponibilité des réseaux. L'implémentation d'une solution de gestion des réseaux totale fait l'objet d'une approche par cycle de vie, qui comprend les étapes suivantes :

- **Evaluation** : identification des manques
  Evaluations complètes, telles que l'évaluation Event-to-Resolution Readiness Assessment, afin de valider le niveau de maturité et d'efficacité actuel de la gestion des performances et de la disponibilité du réseau.
- **Conception :** création de la solution appropriée
  Les architectes CA conçoivent de bonnes solutions de disponibilité des services pour les moyennes entreprises monosites comme pour les organisations informatiques internationales qui exigent une disponibilité 24/24 h et 7/7 j et de très hautes performances.
- **Implémentation :** facteur décisif de succès de la solution
  Les consultants CA préparent l'environnement ; ils installent *e*Health et SPECTRUM, configurent et personnalisent ces produits ; ils vérifient les solutions *e*Health et SPECTRUM et les documentent à partir de systèmes de test, d'assurance qualité et de production ; ils assurent le transfert des connaissances à votre personnel.
- **Optimisation :** anticipation des changements
  Les services d'optimisation évaluent les diverses manières dont vos solutions *e*Health et SPECTRUM peuvent être exploitées ou ajustées. Les services de contrôle d'*e*Health peuvent inclure l'ajustement, la reconfiguration, les mises à niveau et les migrations, ainsi que la formation et les certifications.

Grâce à la solution de gestion de la voix et des réseaux convergents de CA, le service informatique adopte une gestion plus proactive (et non réactive) de la voix et des données. Les équipes chargées d'exploiter les réseaux disposent des outils adéquats pour déterminer rapidement la cause des problèmes. Le groupe d'ingénierie ou de planification informatique peut déterminer si les ressources sont sous-exploitées ou atteignent un seuil de capacité. Le service informatique peut gérer les relations avec les principaux demandeurs à l'aide de niveaux de service formels. Pour bien gérer les niveaux de service, il est essentiel de pouvoir surveiller et signaler la qualité d'écoulement du trafic (GoS, grade of service) et la qualité de service (QoS, quality of service) des appels dans le réseau de voix. C'est possible avec la solution de gestion des réseaux et de la voix de CA.



Chapitre 2 : Défis liés à la gestion des réseaux et de la voix

Toute l'infrastructure informatique (macro-ordinateur, client-serveur, système réparti, grille ou services Web) dépend de la fonction du réseau sur lequel elle réside. Les entreprises sont aujourd'hui conscientes des corrélations entre les services vitaux propres à leur métier, tels que les applications financières et la voix, et l'infrastructure réseau. La lenteur ou le dysfonctionnement de ces infrastructures se traduit par une perte de revenus, une augmentation des coûts et une baisse de productivité tant au niveau des applications et services vitaux que des utilisateurs finals. En moyenne, Infonetics estime que le coût des temps d'arrêt et des dégradations de l'infrastructure représente 3,6 % du chiffre d'affaires annuel des entreprises.[1]

Evolution du réseau en plate-forme de fourniture de service

La nature même des réseaux n'a cessé d'évoluer au cours de ces dernières années, entraînant d'importantes répercussions sur les logiciels de gestion réseau et sur leurs utilisateurs, à savoir les équipes informatiques et celles chargées de l'exploitation des réseaux. Jusqu'à très récemment, la fonction principale des réseaux consistait simplement à maintenir la connectivité des données.

Aujourd'hui, le réseau est davantage considéré comme une plate-forme de fourniture de services. Il prend en charge des services en temps réel tels que la voix sur IP (VoIP), la télévision sur IP (IPTV) et la visioconférence, dont l'utilisation est de plus en plus répandue. Les entreprises s'appuient de plus en plus sur une répartition géographique globale de leurs applications afin de permettre à leurs employés, clients et partenaires d'effectuer à tout moment des tâches vitales. En outre, les équipements réseau sont désormais dotés de services (sécurité, haute disponibilité, stockage, etc.) jusqu'alors pris en charge par des infrastructures extérieures au réseau.

Impact sur les équipes chargées d'exploiter les réseaux

Cette évolution a eu un impact considérable sur les rôles et les responsabilités des équipes chargées d'exploiter les réseaux. Les entreprises s'appuient sur des services en temps réel pour augmenter leurs revenus, améliorer leur productivité et réduire leurs coûts. Toute dégradation d'un service se répercute immédiatement sur le niveau de satisfaction des clients et sur les activités de ces entreprises.

---

[1]Infonetics Research, *The Cost of Enterprise Downtime, North America 2004*. http://www.infonetics.com (Utilisé avec autorisation).



Les applications réseau influent directement sur les résultats des entreprises. De fait, le nombre d'intervenants internes souhaitant comprendre les performances des réseaux n'a cessé d'augmenter : aux équipes techniques s'ajoutent désormais les équipes non techniques, les gestionnaires orientés métier et ceux des secteurs d'activités. Les équipes chargées d'exploiter les réseaux doivent démontrer leur aptitude à répondre aux exigences en termes de niveaux de service à de nouveaux groupes d'utilisateurs (clients internes et externes). Ces utilisateurs n'étant pas des techniciens, ces équipes doivent employer des termes commerciaux plutôt que techniques.

En outre, en raison de l'étroite interdépendance entre infrastructures réseau et applications et services, les équipes chargées d'exploiter les réseaux doivent superviser non seulement ces infrastructures, mais également les applications, la voix et les autres services. Cette supervision requiert une connaissance plus approfondie des nouvelles technologies auparavant gérées par d'autres équipes. L'incorporation de services aux équipements réseau se traduit par une diversification des périphériques, dont la nature complexe rend le travail des équipes réseau encore plus difficile.

Impact sur la configuration logicielle requise pour la gestion des réseaux

L'évolution des défis liés aux réseaux convergents et à l'exploitation réseau exige des solutions de gestion permettant de maintenir la connexion entre les entreprises et les clients internes et externes. L'utilisation stratégique des fonctions de gestion réseau permet de limiter les problèmes de responsabilité entre les gestionnaires réseau et les responsables informatiques ou d'applications. Un groupe doit se charger des problèmes de performances réseau, tandis que l'autre est responsable du bon fonctionnement des applications déployées sur le réseau et de la satisfaction des clients internes qui utilisent ces applications.

Il est essentiel de pouvoir fournir une multitude de rapports et de statistiques sur l'état du réseau. Les outils de gestion réseau simples et conviviaux sont désormais acceptés et pris en compte dans le budget informatique. Ils sont dotés de tableaux de bord d'alertes de haut niveau, ainsi que de fonctions d'analyse détaillée des problèmes liés aux applications et au réseau.

La convergence des réseaux dans l'entreprise et chez les fournisseurs de services oblige les gestionnaires réseau et les responsables informatiques à étudier les conditions réseau pour chaque application et pour chaque flux. La gestion des réseaux locaux sans fil, des systèmes de sécurité, des protocoles VoIP et la configuration réseau offrent déjà de nouvelles opportunités. Les fournisseurs de services gérés doivent disposer d'outils d'automatisation et de visibilité afin de proposer des services sur plusieurs réseaux à une multitude de bureaux. Cette nécessité est amplifiée par la chaîne logistique étroite des réseaux d'information et par la tendance accrue vers une main d'oeuvre mobile et disséminée.



Les équipes d'exploitation responsables de la maintenance des réseaux convergents doivent relever d'importants défis :

- **Réseaux hétérogènes.** Les réseaux sont constitués d'un large éventail de technologies et de fournisseurs, notamment des technologies de données (IP, ATM, FR, transmission à large bande, etc.), ainsi que des infrastructures de voix intégrant l'héritage du multiplexage par répartition dans le temps (MRT), la téléphonie sur IP analogique et des infrastructures hybrides. En règle générale, la migration vers la VoIP s'effectue de manière progressive ; par conséquent, il est toujours nécessaire de gérer simultanément les environnements de MRT et de téléphonie IP.
- **Echelle.** Les infrastructures de voix et de données s'étendent sur de larges zones géographiques. Elles peuvent couvrir plusieurs fuseaux horaires, pays, voire continents. Le système de gestion doit être capable de s'adapter à ces très grandes infrastructures et fournir les informations requises aux équipes chargées de l'exploitation, qu'elles soient centralisées ou réparties dans diverses régions.
- **Nécessité de gérer les infrastructures de données, de voix et les systèmes vitaux.** Le système de gestion doit couvrir plusieurs domaines, afin que les équipes informatiques puissent gérer correctement les domaines techniques qui étaient auparavant traités par des experts.
- **Nécessité d'informer divers intervenants de la qualité de service.** Les équipes chargées de l'exploitation doivent être en mesure de diffuser des informations aux clients externes par le biais des contrats de niveau de service et aux intervenants internes par l'intermédiaire des contrats de niveau d'exploitation ou de mécanismes moins formels. Les logiciels de gestion doivent, par conséquent, proposer des fonctionnalités intelligentes pour répondre aux besoins des techniciens et des utilisateurs orientés métier :
    - Evaluer la capacité de l'infrastructure à soutenir l'activité
    - Identifier les problèmes dès qu'ils surviennent
    - Mettre en évidence la source ou la cause des problèmes

En réponse à ces tendances, le marché de la disponibilité des réseaux à travers le monde enregistre une croissance rapide. Grâce à des logiciels de gestion réseau performants, les entreprises disposent désormais d'outils nécessaires pour améliorer leur efficacité.



(Page laissée intentionnellement vide)



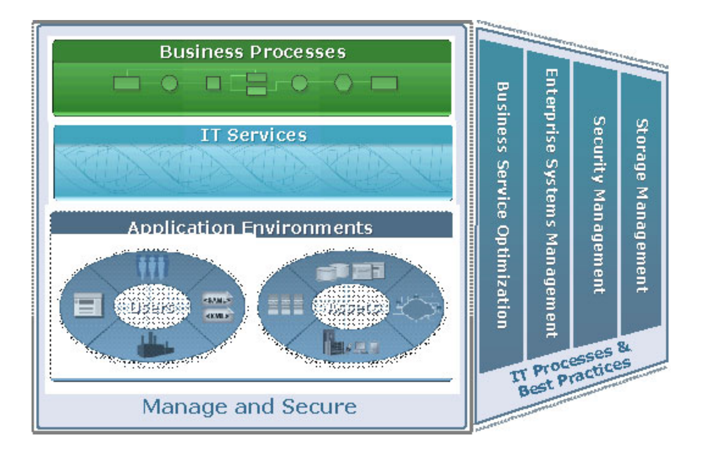
Chapitre 3 : Solution de gestion des réseaux et de la voix de CA

EITM : l'approche de CA

L'approche EITM, démarche de gestion et de sécurisation dynamiques des environnements informatiques de CA, permet aux entreprises de concrétiser tout le potentiel commercial de leurs systèmes informatiques. EITM fournit une base commune d'intégration et de partage des services et des données, permettant une orchestration homogène de toutes les ressources informatiques (infrastructure, applications et processus métier). Cette approche orientée métier intègre également la gestion des réseaux, des systèmes, du stockage, des bases de données, des applications et de la sécurité. Elle offre en outre un moyen innovant de mesurer, optimiser et démontrer l'impact de l'informatique sur les objectifs de l'entreprise.

CA est le premier fournisseur mondial de solutions de gestion. Depuis plus de 30 ans, nous jouons un rôle actif sur le marché des logiciels de gestion et offrons des solutions ciblées dans tous les domaines de la gestion d'infrastructures. Nous aidons les entreprises à atteindre leurs objectifs de réduction de coûts informatiques et de rentabilisation des investissements et des dépenses liées à l'exploitation, tout en limitant les risques et en assurant le fonctionnement optimal des infrastructures conformément à la réglementation en vigueur.

L'approche de CA est centrée sur l'offre de solutions de gestion proposant une vision unifiée de toutes les ressources et opérations de l'entreprise en fonction des activités et des besoins. Cette vision permet aux entreprises d'aligner l'informatique sur l'activité, ce qui assure une prise de décision plus efficace et mieux informée sur l'orientation des activités et sur l'utilisation des ressources.



Service Availability (SA) figure parmi les solutions de gestion de CA. SA permet de fournir des services informatiques stables et de haute qualité grâce à l'implémentation d'une gestion intégrée et proactive qui offre un aperçu du fonctionnement des systèmes et applications dont dépend chaque service métier.



Gestion des systèmes d'entreprise

Alors que les entreprises développent leurs activités afin d'élargir leur clientèle et de consolider leur avantage concurrentiel, une nouvelle génération de solutions de gestion des réseaux et des systèmes a été mise au point pour les aider à adopter une approche plus proactive et orientée services, et d'optimiser ainsi la disponibilité et les performances des processus métier. Ces solutions permettent de réduire ou de minimiser les risques tout en augmentant l'efficacité opérationnelle, la continuité des activités et le respect des réglementations, ce qui aboutit à des services informatiques rentables adaptés à l'activité.

Grâce à leur performance et à leur souplesse, les solutions de gestion des systèmes d'entreprise fournissent des services informatiques adaptés aux activités des entreprises et aux besoins métier. Elles doivent permettre d'adapter les ressources informatiques aux besoins de l'entreprise en fonction de l'impact sur l'activité. L'automatisation, telle que définie par les stratégies, est au coeur des solutions de gestion des systèmes d'entreprise de CA.

Les services informatiques sont chargés d'assurer l'exploitation correcte, le bon fonctionnement, les performances et un niveau acceptable de disponibilité des infrastructures. Les solutions de gestion des systèmes d'entreprise de CA vous aident à atteindre ces objectifs grâce à :

- La gestion des réseaux et systèmes à des fins de disponibilité et de performance
- L'automatisation des jobs et événements à des fins d'optimisation
- La gestion des applications et bases de données à des fins de performances
- L'approvisionnement et configuration de PC et de serveurs

Pour CA, la gestion d'entreprise n'est pas compatible avec le concept d'isolement et doit s'intégrer dans une infrastructure informatique globale couvrant plusieurs disciplines. Les serveurs se révèlent utiles uniquement dans la mesure où ils fonctionnent de manière fiable sur des réseaux supposés très performants. De même, les applications offrent le même niveau de sécurité que les systèmes qui en contrôlent l'accès. En outre, le fonctionnement de l'infrastructure est correct uniquement en présence de systèmes de stockage qui répondent aux besoins de l'entreprise.

L'approche de CA repose sur la croyance selon laquelle des disciplines traditionnellement distinctes (réseaux et systèmes, stockage, sécurité et gestion des services) doivent être étroitement combinées afin d'optimiser les performances, la fiabilité et l'efficacité des environnements informatiques d'entreprise. CA a conçu des produits qui interagissent les uns avec les autres, en exploitant des composants logiciels de services communs qui exécutent des fonctions réutilisables dans plusieurs applications. En développant une base de données de gestion centrale afin d'offrir une vue unifiée de tous les aspects de l'entreprise en rapport avec ses activités et ses besoins, CA a posé les bases d'un service informatique centré sur le métier.



Les services informatiques comprennent parfaitement la façon dont toutes leurs ressources informatiques sont utilisées, car ils ont accès à des informations interdisciplinaires complètes. Munis de ces connaissances, ils peuvent offrir des services tout particulièrement adaptés aux besoins de chaque service technique et fournir aux responsables des commentaires sur l'utilisation des ressources informatiques et sur leurs coûts induits. Les décideurs sont ainsi à même de choisir en toute connaissance de cause l'orientation à donner à leurs activités.

Avantages de la solution de gestion des réseaux et de la voix de CA

Les entreprises d'aujourd'hui considèrent qu'il est essentiel de posséder des solutions de données et de voix très performantes pour qu'elles soient compétitives. L'approche de CA en matière de gestion convergente de la voix et des données permet aux services informatiques de gérer de bout en bout les services de voix et de données de manière proactive, d'assurer une capacité suffisante pour la bande passante et les systèmes et de prendre en charge les niveaux de service définis par l'entreprise. La solution de gestion des réseaux et de la voix de CA englobe les technologies IP et traditionnelles, ce qui permet aux entreprises de passer à la téléphonie IP à leur rythme et de réduire la complexité inhérente à la gestion d'infrastructures hétérogènes. Nous implémentons cette approche dans notre stratégie produit via la mise à jour, l'innovation et l'intégration des produits, conformément aux exigences de nos clients.

La solution de gestion des réseaux et de la voix de CA offre les principaux avantages suivants :

- **Gestion efficace des niveaux de service.** Définit des lignes de référence, évalue et assure le suivi des services du réseau. Diffuse des informations sur le respect des contrats de niveau de service et d'exploitation auprès des utilisateurs orientés métier et des techniciens.
- **Assurance proactive des services.** Les fonctions de surveillance, définies par des stratégies, servent à identifier les dégradations de services avant qu'elles ne se répercutent sur les clients. Ces dégradations sont ensuite soumises aux processus d'analyse de la cause première (RCA) et de corrélation des événements.
- **Détection rapide des problèmes.** Elimine la véritable cause du problème (et non les symptômes) grâce aux fonctions de corrélation des événements, d'analyse de la cause première et de liaison avec la génération de rapports historiques et en temps réel.
- **Planification prédictive de la capacité.** Des algorithmes intelligents intégrés informent les équipes chargées de l'exploitation réseau de la date de mise à niveau ou de rétrogradation des circuits ou autre matériel en fonction des tendances d'utilisation antérieures et des seuils définis.

Notre stratégie de gestion des réseaux et de la voix comporte quatre volets :

- Permettre à nos clients de gérer leurs processus métier, ainsi que les services multimédias, de données et de voix, conformément à leur stratégie commerciale
- Permettre à nos clients de gérer leurs réseaux convergents, notamment les applications vitales, ainsi que la transition vers la téléphonie IP
- Permettre la gestion de bout en bout des défaillances et des performances pour les infrastructures de données, de voix (MRT et téléphonie IP), les systèmes et les applications
- Etendre la gestion aux ressources de voix et multimédia, ainsi qu'à l'infrastructure réseau



CA propose des solutions uniques :

- Une solution de gestion proactive intégrée
- Une solution qui englobe les technologies IP et traditionnelles
- Des solutions qui garantissent les performances des réseaux de voix avant, pendant et après une migration vers la VoIP

Grâce à la solution de gestion des réseaux et de la voix de CA, le service informatique passe à une gestion plus proactive (et non réactive) de la voix et des données. Par exemple, au lieu d'attendre que les clients se plaignent d'une mauvaise qualité de la voix pour agir, le personnel informatique reçoit des alertes lorsque des stratégies indiquant une faible gigue, un faible taux MOS ou des problèmes matériels tels que des circuits T1 dépassant des seuils utilisateur prédéfinis. Lorsqu'un problème survient dans un environnement de téléphonie IP, il est parfois difficile d'en déterminer la cause. Par exemple, un utilisateur peut se plaindre de ne pas pouvoir passer d'appel, alors que plusieurs événements d'alarme peuvent être générés par des routeurs, des systèmes de téléphonie IP, des commutateurs, etc. La solution de gestion des réseaux et de la voix de CA permet une gestion proactive de la téléphonie et de la voix sur IP.

La planification de la capacité est essentielle à la gestion convergente des données et de la voix. Les données collectées à partir des systèmes de voix, qu'ils soient traditionnels ou IPT, et à partir du réseau (notamment la capacité des jonctions et des ports) permettent aux ingénieurs informatiques de déterminer si des ressources sous-exploitées atteignent un seuil de capacité. La planification prédictive de la capacité du réseau peut également s'appuyer sur ces informations. Les services informatiques sont chargés de fournir des niveaux de service aux principaux demandeurs, notamment aux unités commerciales génératrices de revenus, telles que les centres d'appels. La gestion des niveaux de service repose essentiellement sur la capacité à surveiller la qualité d'écoulement du trafic et la qualité de service des appels dans le réseau de voix et à consigner ces éléments dans des rapports.

Elément clé de l'approche EITM de CA

La solution de gestion des réseaux et de la voix de CA s'intègre dans la stratégie d'entreprise EITM de CA. La solution répond aux quatre impératifs principaux des responsables informatiques, comme suit :

- Elle améliore le service en fournissant une assurance proactive des services afin de détecter les problèmes avant qu'ils ne se répercutent sur les utilisateurs finals. Elle garantit la fiabilité et la réactivité de l'infrastructure réseau avec de puissantes fonctions d'analyse de la cause première, de corrélation des événements et d'analyse d'impact.
- Elle gère les risques en assurant la continuité des activités, permettant ainsi aux organisations de respecter les exigences réglementaires et gouvernementales.
- Elle réduit considérablement le coût des temps d'arrêt (interruption ou dégradation) en limitant le nombre de temps d'arrêt et leur durée.
- Elle adapte l'informatique à l'activité en offrant à l'équipe informatique la possibilité de visualiser l'état du service métier de bout en bout.



Gestion des réseaux et de la voix pour les principaux marches verticaux

CA fournit un logiciel de gestion puissant et unique qui permet de gérer des services réseau de plus en plus complexes dans des environnements traditionnels et gouvernementaux ainsi que dans les industies de télécommunication, du câblage, de la technologie sans fil mobile et d'autres secteurs de fourniture de services. Il permet aux équipes techniques d'améliorer la qualité de leurs services, de maîtriser les coûts, de réduire les risques, d'augmenter les revenus et d'accroître leur efficacité lorsqu'elles gèrent l'infrastructure informatique comme un service métier.

Fournisseurs de services de télécommunication

CA considère la fourniture de services de télécommunication comme un important marché vertical dont leurs membres exploitent un environnement opérationnel principalement afin de maîtriser les coûts et d'offrir des produits/services différents. Ces facteurs sont essentiels pour rester compétitif dans un secteur de communications exigeant.

La plupart des fournisseurs de services choisissent divers outils de gestion spécifiques à la gestion d'éléments, à l'approvisionnement de services, à la facturation, à l'assistance clientèle et à l'assurance de services. Dans de grands environnements de fourniture de services et de transport, ce choix crée de nombreuses applications et données disparates. Celles-ci doivent être en quelque sorte intégrées dans des processus de workflow efficaces pour garantir une livraison fiable des services tout en maintenant l'efficacité opérationnelle. La solution de gestion des réseaux et de la voix de CA contient des points d'intégration souples pour fonctionner correctement dans des environnements logiciels OSS (Operational Support System, système de soutien des opérations) hétérogènes, tout en réduisant la durée et la complexité du déploiement, ainsi que les coûts de configuration et de maintenance. CA collabore avec les principaux fournisseurs OSS dans les domaines de l'assurance des services, de l'exécution, de la facturation et de l'assistance clientèle.

Grâce à la solution de gestion des réseaux et de la voix de CA, les fournisseurs de services peuvent atteindre les objectifs suivants :

- Vérifier les garanties des contrats de niveau de service et les valider afin d'améliorer la satisfaction et la fidélisation des clients.
- Réduire les frais d'exploitation en limitant le temps d'arrêt et le délai moyen de réparation.
- Réduire les dépenses de capital via la planification intelligente de la capacité.
- Accélérer la prise en charge des nouvelles offres de service :
    - Réseau privé virtuel (RPV)
    - VoIP
    - Service trois en un de voix/vidéo/données
    - Nouveaux services de données sans fil



Gouvernement

L'utilisation de produits CA est largement répandue auprès des gouvernements nationaux et locaux à travers le monde. La solution de gestion des réseaux et de la voix de CA aide les agences civiles et militaires à satisfaire leurs besoins d'automatisation des opérations informatiques en proposant des fonctions pratiques et réalisables qui assurent un retour sur investissement rapide et la réussite des missions. Déployée sur des camions ou sur d'autres véhicules mobiles, elle garantit les performances et la fiabilité des communications par IP, satellite, radio, faisceaux hertziens et téléphoniques entre les premières lignes et les donneurs d'ordre dans des postes opérationnels éloignés. CA offre des fonctionnalités uniques en faveur d'initiatives militaires centrées sur le réseau et de la gestion et du traitement des informations électroniques.

Entreprise

L'utilisation de la solution de gestion des réseaux et de la voix de CA est largement répandue dans les marchés verticaux suivants : industrie automobile, manufacturière, pharmaceutique et de l'accueil, éducation, énergie, divertissement, consommation, services financiers, santé, vente au détail, semi-conducteurs, technologie et transport. Tous ces secteurs sont fortement influencés par les temps d'arrêt.

Les réseaux convergents de données et de voix actuels doivent notamment permettre de gérer de bout en bout l'infrastructure de données, ainsi que les systèmes et services de messagerie vocale. Pour ce faire, la solution doit assurer la gestion des performances et des défaillances du réseau, de la voix (autocommutateurs privés, systèmes de messagerie et autres services de voix) et du système afin que les équipes chargées de l'exploitation réseau puissent gérer les systèmes vitaux placés sous leur responsabilité.

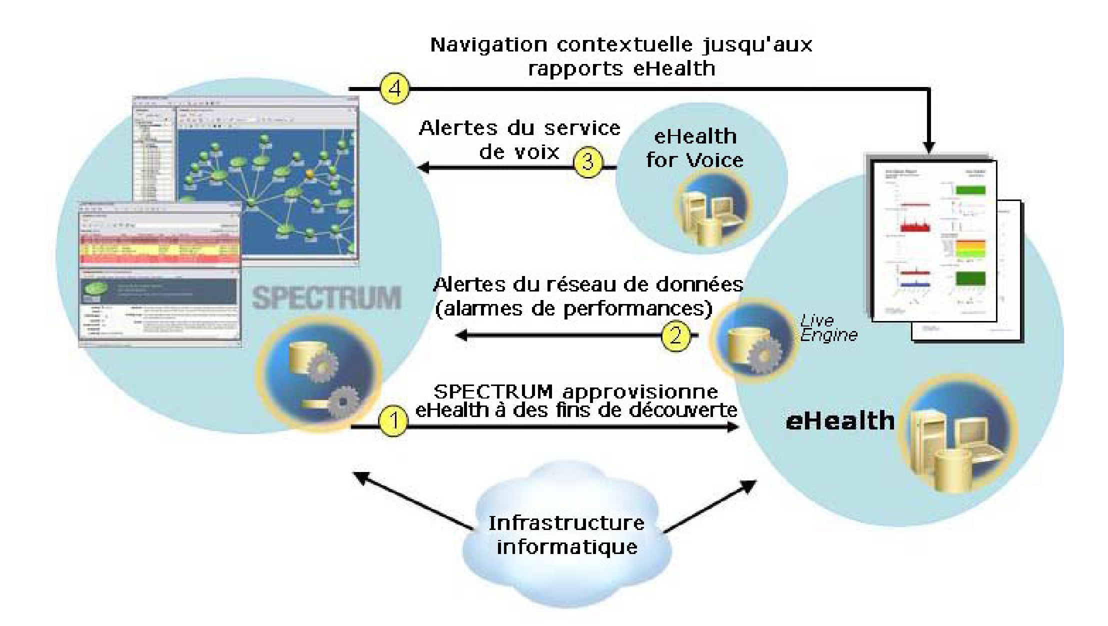
Composants de la solution

Sur ce marché, la solution CA comporte trois principales gammes de produits, chacune offrant un ensemble homogène de fonctions destinées à l'infrastructure de données et de voix :

- ***e*Health** évalue l'intégrité du réseau et détermine s'il peut prendre en charge la voix. Ce module décrit le fonctionnement du réseau, vous permet de comparer la note moyenne d'opinion sur la voix avec les statistiques sur la qualité de service et identifie les tendances en termes de performances.
- **SPECTRUM** permet la gestion des défaillances, l'analyse de la cause première et la modélisation de la voix. Il vous permet également de modéliser les composants de vos services de voix pour garantir un fonctionnement normal de ces services.
- ***e*Health for Voice** offre des fonctions de gestion des performances pour les systèmes de communication (IP et MRT traditionnels), les systèmes de messagerie et permet la gestion de tous les aspects liés à la téléphonie.



Ces applications peuvent fonctionner en tant que systèmes autonomes ou intégrés, comme indiqué ci-dessous.



*e*Health

eHealth vous aide à maîtriser les performances réseau et à garantir la qualité de service (QoS) dans toute l'infrastructure du réseau. Vous pouvez ainsi exécuter une multitude de tâches telles que la vérification de la disponibilité et des performances du réseau, la documentation des niveaux de service, la gestion de la capacité et la planification exacte de la croissance. Cette solution vous permet de relever de nombreux défis, parmi lesquels la gestion d'un ensemble diversifié de périphériques provenant d'un grand nombre de fournisseurs, l'isolation de la source de détérioration des performances sur le réseau, la réduction des dépenses récurrentes liées au réseau étendu et la génération de rapports cohérents dans toute votre infrastructure de réseaux hétérogènes.

Ce composant de la solution vous permet d'atteindre les objectifs suivants :

- Améliorer la disponibilité des services de votre réseau
- Réduire le coût des temps d'arrêt et l'impact de ce dernier sur l'utilisateur final
- Identifier et résoudre les problèmes plus rapidement
- Planifier préventivement la capacité
- Améliorer la qualité de service
- Respecter et s'engager sur des niveaux de service



Composants d'*e*Health

*e*Health comprend les composants suivants :

- *e*Health E2E Console
- *e*Health Live Health
- *e*Health Traffic Accountant
- Report Center
- Distributed *e*Health
- *e*Health SPECTRUM Integration
- *e*Health Universal Workflow Integration Modules (HP OpenView, IBM (Micromuse), Netcool, Cisco CIC)
- *e*Health Universal Data Integration Modules (Cisco WAN Manager, Cisco IP Solution Center, Lucent, Nortel, Alcatel)
- *e*Health Universal Wireless Integration Modules (Nortel, Starent)

Avantages d'*e*Health

*e*Health se distingue des autres solutions sur les points suivants :

- *e*Health offre la meilleure gestion proactive de sa catégorie, de sorte que les services informatiques peuvent résoudre les problèmes avant qu'ils n'aient un impact sur le chiffre d'affaires.
- Il prend en charge le plus grand éventail de produits : plus de 1 000 périphériques provenant de 100 fournisseurs différents.
- Ses rapports sont dotés d'une intelligence intégrée permettant de résoudre les problèmes sans avoir besoin de connaître parfaitement chaque composant du service.
- *e*Health crée des références automatiques, c'est-à-dire qu'il étudie le comportement normal de chaque périphérique de gestion. L'algorithme d'écart par rapport à la normale offre un seuil plus précis par rapport à l'historique car il compare les valeurs de performances actuelles à la tendance la plus récente dans une fenêtre d'analyse spécifique.
- Contrairement à CA, de nombreux fournisseurs assurent une prise en charge limitée des technologies et des périphériques, ce qui pose problème aux entreprises qui tentent de réduire le nombre de fournisseurs en logiciels de gestion.
    - Les clients attendent davantage de responsabilités de la part de leurs fournisseurs, étant donné que l'informatique est plus qu'un simple service.
    - La diminution du nombre de fournisseurs réduit la complexité, les frais d'exploitation et les risques de déployer de nouvelles initiatives métier.
- La valeur d'une plate-forme de gestion intégrée est significative puisque les services informatiques consacrent beaucoup de temps et d'argent à identifier la cause des problèmes, et les temps d'arrêt de service coûtent extrêmement cher.



SPECTRUM

SPECTRUM est capable de gérer des réseaux au niveau local comme à l'échelle internationale. Il fournit une visibilité granulaire des couches 2 et 3 jusqu'à chaque port et circuit d'un réseau local, étendu, câblé, sans fil, physique ou virtuel. Il offre des applications de gestion spécifiques permettant d'effectuer un zoom avant pour surveiller et analyser les technologies de mode de transfert asynchrone (ATM, asynchronous transfer mode), de relais de trame, de multidiffusion du protocole Internet, de qualité de service, de la voix et VPN. Sa technologie brevetée d'analyse d'impact et de la cause première identifie l'emplacement exact des périphériques endommagés ou en échec.

Ce composant de la solution vous permet d'atteindre les objectifs suivants :

- Gérer la disponibilité des services de votre réseau
- Identifier la cause première d'un échec du réseau
- Observer les relations et l'impact des infrastructures informatiques sur les services métier
- Consulter l'état des opérations affectées
- Assurer l'intégrité opérationnelle de l'infrastructure en assurant le suivi des modifications apportées à celle-ci

Composants de SPECTRUM

SPECTRUM comprend les composants suivants :

- SPECTRUM Infinity
- SPECTRUM Integrity
- SPECTRUM Xsight
- SPECTRUM OneClick
- SPECTRUM Service Manager
- SPECTRUM Report Manager
- SPECTRUM Alarm Notification Manager
- SPECTRUM ATM Circuit Manager
- SPECTRUM Configuration Manager
- SPECTRUM Secure Domain Manager
- SPECTRUM Frame Relay Manager
- SPECTRUM Microsoft Operations Manager Connector
- SPECTRUM Multicast Manager
- SPECTRUM OSS Integrations
- SPECTRUM QoS Manager
- SPECTRUM Remedy ARS Gateway
- SPECTRUM SNMPv3 Support
- SPECTRUM VPN Manager
- SPECTRUM Watch Editor
- SPECTRUM Service Performance Manager



Avantages de SPECTRUM

SPECTRUM se distingue des autres solutions selon les points suivants :

- SPECTRUM offre des fonctions inégalées d'analyse de la cause première et d'accès à la base de connaissances de la solution SPECTRUM :
  - Identification plus rapide de la cause première des problèmes informatiques
  - Recherche accélérée des fausses alertes et alarmes
  - Elimination des problèmes de responsabilité et des rejets de responsabilité
- Les services informatiques peuvent encore tirer parti de la fonction avancée d'analyse de la cause première grâce au système Event Management (EMS) ou à la corrélation des conditions, tous deux basés sur des stratégies, et non à la technologie de modélisation inductive basée sur le modèle (IMT).
- Il anticipe et évite les problèmes dès sa première utilisation en proposant des seuils intelligents. Les autres solutions identifient uniquement les problèmes après leur apparition.

Intégration entre *e*Health et SPECTRUM

L'intégration entre *e*Health et SPECTRUM combine le meilleur de la gestion des défaillances et des performances réseau pour offrir une solution complète garantissant une disponibilité et une réactivité élevées de vos réseaux de données vitales. Elle permet aux clients d'atteindre les objectifs suivants :

- Intégrer à SPECTRUM des alarmes Live Health et d'exception de rapports de santé, qui apparaissent ensuite dans l'interface SPECTRUM OneClick.
- Fournir un lancement contextuel à partir des vues d'alarme et de topologie SPECTRUM vers les rapports *e*Health.
- Permettre l'utilisation de fichiers SPECTRUM dans la découverte d'*e*Health.

*e*Health for Voice

*e*Health for Voice offre une gestion complète des services de voix sur le réseau, notamment les autocommutateurs privés, la téléphonie IP, la messagerie vocale, la messagerie unifiée et l'utilisation de la bande passante.

Ce composant de la solution vous permet d'atteindre les objectifs suivants :

- Consolider les informations à partir de plusieurs composants système et réseau, qu'ils soient traditionnels ou basés sur IP, pour proposer une vue complète du système de voix et des performances réseau.
- Automatiser la collecte de données ou le processus d'interrogation à partir de périphériques traditionnels par le biais d'un modem, de l'IP ou de systèmes d'accès sécurisés.
- Identifier les composants de l'infrastructure de téléphonie IP.
- Gérer les stratégies de qualité de services du trafic de voix.
- Surveiller les passerelles de voix, les processeurs de signaux numériques (DSP) et la communication poste à poste.
- Estimer la note moyenne d'opinion entre les extrémités du routeur.
- Obtenir une vision de bout en bout de la qualité, de la gigue et du retard de la voix.



*e*Health for Voice vous permet d'obtenir une vue globale des systèmes de voix, des réseaux et des services afin de gérer efficacement les niveaux de service. Il vous permet aussi d'effectuer un zoom avant sur les détails pour garantir une capacité suffisante, une analyse de la cause première et une assurance proactive des services.

Avantages d'*e*Health for Voice

*e*Health for Voice offre les avantages suivants :

- Permet de gérer les processus métier, y compris les services de voix et multimédias, en cohérence avec votre stratégie commerciale.
- Permet de gérer la transition entre la téléphonie traditionnelle et IP.
- Offre une gestion de bout en bout des performances et des défaillances des réseaux de téléphonie IP.
- Gère les ressources de voix et multimédias pour réduire les risques, maîtriser les coûts, activer de nouveaux services et aligner vos investissements avec vos objectifs informatiques.

Offres de services de gestion de réseaux et de voix de CA Technology Services

CA Technology Services emploie des experts d'*e*Health et de SPECTRUM qui aident les entreprises à évaluer, concevoir, implémenter et optimiser des solutions de disponibilité et de performances du réseau et de la voix dans toute leur infrastructure. Des fournisseurs de services financiers aux organismes gouvernementaux et autres, en passant par les entreprises de télécommunications, les experts de CA vous aident à établir les workflows recommandés, à intégrer vos solutions de gestion réseau et à combiner vos solutions de disponibilité et de performances réseau et de la voix avec votre centre de services afin d'obtenir un système de gestion des événements réseau consolidé.

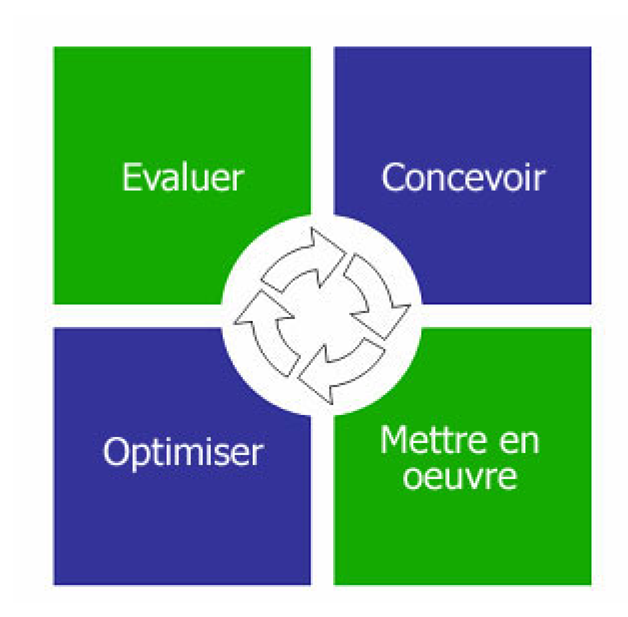
La mission des experts en performances et disponibilité du réseau et de la voix de CA consiste à vous permettre d'atteindre les objectifs suivants :

- **Améliorer l'alignement des besoins métier** en associant l'infrastructure réseau à des services informatiques vitaux qui prennent en charge l'activité et en garantissant que l'équipe réseau se concentre sur les services les plus importants pour l'entreprise.
- **Augmenter les capacités de planification de l'entreprise** en offrant une vision complète de l'infrastructure réseau grâce à des consoles, des rapports et des analyses des mesures consolidés.
- **Réduire les risques** en définissant et en implémentant des réparations automatiques qui évitent les possibilités d'erreur humaine et garantissent une résolution des problèmes homogène.
- **Maîtriser les coûts** en consolidant la gestion des événements du réseau en un point de contrôle central, ce qui réduit les besoins de dotation en personnel.
- **Rentabiliser les systèmes de gestion réseau existants** en intégrant vos principaux outils et workflows et en les superposant.
- **Optimiser la fourniture des services informatiques** en appliquant les normes ISO et CobiT, les recommandations de l'ITIL et les processus de gestion réseau éprouvés.



APPROCHE PAR CYCLE DE VIE DES SOLUTIONS DE DISPONIBILITÉ ET DE PERFORMANCES DU RÉSEAU ET DE LA VOIX

Chaque entreprise a des besoins uniques, mais partage des thèmes communs lorsqu'il s'agit de gérer un réseau : les processus et la surveillance des workflows, ainsi que l'instrumentation de la gestion. Une solution CA est déployée et optimisée en fonction des besoins spécifiques de votre entreprise selon un cycle de vie d'offres de services recommandées.



Evaluation : identification des manques

Les évaluations complètes valident la maturité et l'efficacité de la gestion de la disponibilité et des performances du réseau et de la voix. Les experts de CA effectuent une analyse complète des capacités de gestion réseau suivantes :

- Buts, objectifs, capacités et stratégies de gestion du réseau
- Structure organisationnelle de l'exploitation du réseau ; rôles et responsabilités du personnel
- Logiciels d'intégration, de configuration et de surveillance du réseau
- Topologie et conception du réseau
- Simulation du trafic de voix
- Analyse des données
- Contraintes de sécurité associées (pare-feu, listes d'accès, etc.)
- Définition des alarmes/de la gravité des événements
- Défis et problèmes environnementaux, techniques et commerciaux existants
- Modification des processus de contrôle
- Exigences liées à l'intégration des produits CA et tiers

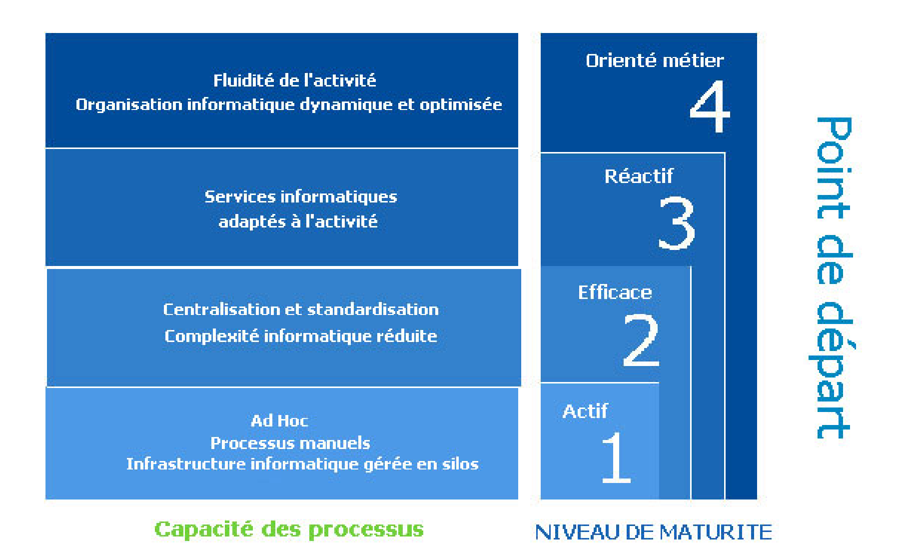


Vos capacités de gestion actuelles sont comparées au modèle de maturité de CA pour les personnes, les processus et les technologies. Les résultats de l'évaluation sont présentés dans un aperçu de l'architecture de la solution (SAO, Solution Architecture Overview). Le SAO est un modèle qui définit les phases réalisables de la solution afin d'optimiser les workflows d'identification et de résolution des problèmes, d'appliquer l'automatisation et d'intégrer les opérations des centres de services. De plus, les consultants et les architectes CA effectuent des recherches, associent l'infrastructure réseau aux services informatiques et donnent des recommandations et des justifications métier vous permettant de justifier votre financement.

Modèles de maturité CA

Les recommandations du secteur ont été associées à quatre phases distinctes de maturité informatique. Les modèles de maturité CA sont conçus pour permettre de :

- Déterminer l'état actuel des processus de gestion informatique
- Evaluer la maturité des capacités informatiques
- Identifier les points faibles des processus et le retour sur investissement résultant de l'amélioration et de l'automatisation de ceux-ci



Conception : création de la solution appropriée

Les architectes CA conçoivent de bonnes solutions de disponibilité et de performances du réseau et de la voix pour les entreprises monosite comme pour les organisations informatiques internationales qui exigent une disponibilité 24/24 h et 7/7 j et de très hautes performances. La valeur ajoutée est issue de l'intégration du centre de services aux réseaux qui prennent en charge les applications, les bases de données, les systèmes, le stockage et la sécurité.

Les architectes collaborent avec les clients pour étudier l'évaluation ou documenter l'environnement « en l'état », mener des entretiens pour garantir l'atteinte des objectifs de gestion informatique et de l'entreprise, établir des corrélations entre les fonctionnalités d'eHealth et de SPECTRUM et vos exigences informatiques et métier et identifier les besoins matériels et de personnalisation. Dans ce processus, les architectes développent un plan de conception et d'implémentation complet, la spécification de l'architecture de la solution (SAS, Solution Architecture Specification).



Les architectes CA doivent être certifiés pour la conception (design). Le processus de qualification des architectes est un programme intensif de deux ans qui requiert plusieurs certifications du secteur, une formation à la technologie de gestion informatique et aux produits CA, ainsi que l'approbation du conseil de l'autorité des architectes CA. Nous exigeons que nos architectes renouvellent leur certification au moins tous les deux ans.

Les clients qui emploient des architectes en interne et gèrent leur propre planification de conception, mais qui peuvent avoir besoin d'une assistance supplémentaire, peuvent tirer parti de la solution Enterprise Systems Management. Ce progiciel expert fournit des conseils de conception à court terme personnalisés ou permet une aide sur un périmètre spécifique.

Implémentation : facteur décisif de succès de la solution

En utilisant SAS comme guide, les consultants CA préparent l'environnement, installent *e*Health et SPECTRUM, configurent et personnalisent ces produits ; ils vérifient les solutions *e*Healh et SPECTRUM et les documentent à partir d'environnements de test, d'assurance qualité et de production ; ils assurent le transfert des connaissances à votre personnel. Les services d'implémentation comprennent également le développement et le déploiement de composants d'intégration entre *e*Health et SPECTRUM, vos autres applications de gestion informatique et votre centre de services.

Pour garantir une gestion stricte des opérations d'implémentation, les chefs de projets certifiés PMP en suivent la progression, les questions, les problèmes et les obstacles. Ils génèrent ensuite les rapports correspondants. CA Technology Services fait appel à des chefs de projets certifiés PMP et à des architectes, des consultants et des partenaires hautement qualifiés. Chaque année, CA Technology Services investit 50 % de plus que la moyenne du secteur dans la formation de nos professionnels.

Optimisation : anticipation des changements

Les services d'optimisation évaluent les diverses manières dont vos solutions eHealth et SPECTRUM peuvent être exploitées ou ajustées. Les services de contrôle de l'intégrité peuvent inclure l'ajustement, la reconfiguration, les mises à niveau et les migrations. D'autres services comprennent la formation et la certification en vue d'améliorer l'efficacité du personnel. L'expérience passée a démontré que la formation du personnel entraînait une exploitation plus efficace. Ces services sont proposés sous la forme de cours dispensés par un formateur sur site ou non, à votre rythme ou sur Internet. Les formateurs ou les personnes qui élaborent les cours sont également des experts certifiés, spécialistes de la disponibilité et des performances du réseau et de la voix.



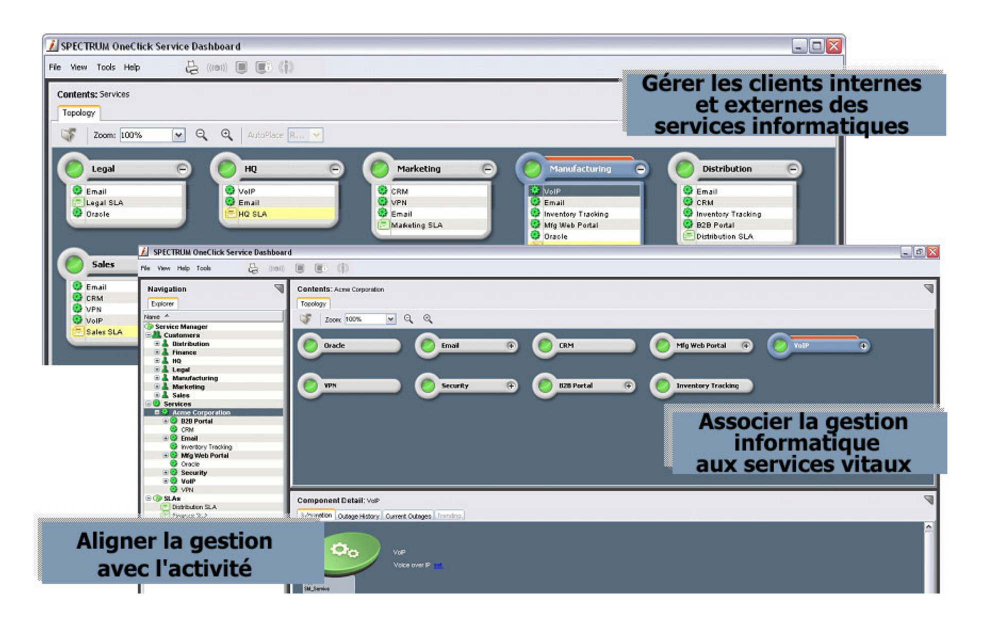
Pourquoi confier la disponibilité de vos services à CA Technology Services ?

- **Expérience** : CA a 30 ans d'expérience en matière de services de gestion de systèmes d'entreprise à son actif.
- **Processus éprouvés** : une équipe d'évaluation dédiée planifie les recommandations de workflow et de réseau, les conçoit en apportant une justification métier et intègre les recommandations dans le modèle de chaque client.
- **Compétences** : une communauté active de professionnels du monde entier, axée sur le réseau, la disponibilité de la voix et les performances, partage leurs connaissances des solutions et contribue sans cesse à l'amélioration des recommandations et modèles de solutions.
- **Objectif** : CA Technology Services se compose d'une équipe de gestionnaires de solutions et d'architectes dédiés, qui se concentrent exclusivement sur les méthodologies d'évaluation, de conception, de livraison et de workflow proposées autour des solutions et des services *e*Health et SPECTRUM.

Mise en application des principaux avantages de la solution

Gestion efficace des niveaux de service

SPECTRUM Service Manager transmet l'état des services vitaux aux gestionnaires d'exploitation et aux non experts du secteur, d'une manière non technique. Les informations concernant l'état des services peuvent être organisées de différentes manières : par service, par division (pour les clients internes) ou par client (pour la communication relative à la gestion des niveaux de service avec les clients externes).

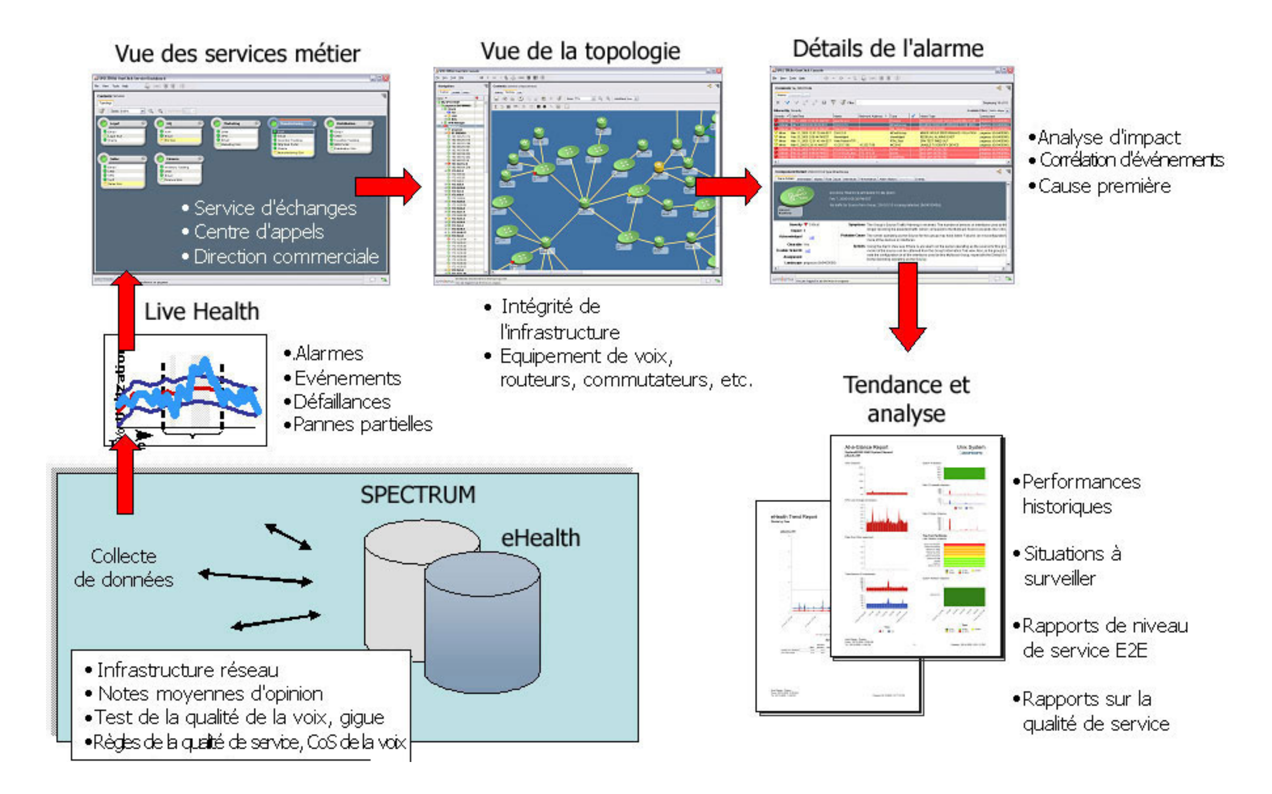


Assurance proactive des services

Les produits de gestion des réseaux et de la voix de CA sont utilisés simultanément pour une assurance proactive des services par le biais des algorithmes intégrés au sein de toutes les gammes de produits. Les équipes chargées de l'exploitation peuvent ainsi identifier les problèmes potentiels AVANT qu'ils n'aient une incidence sur le service clients.



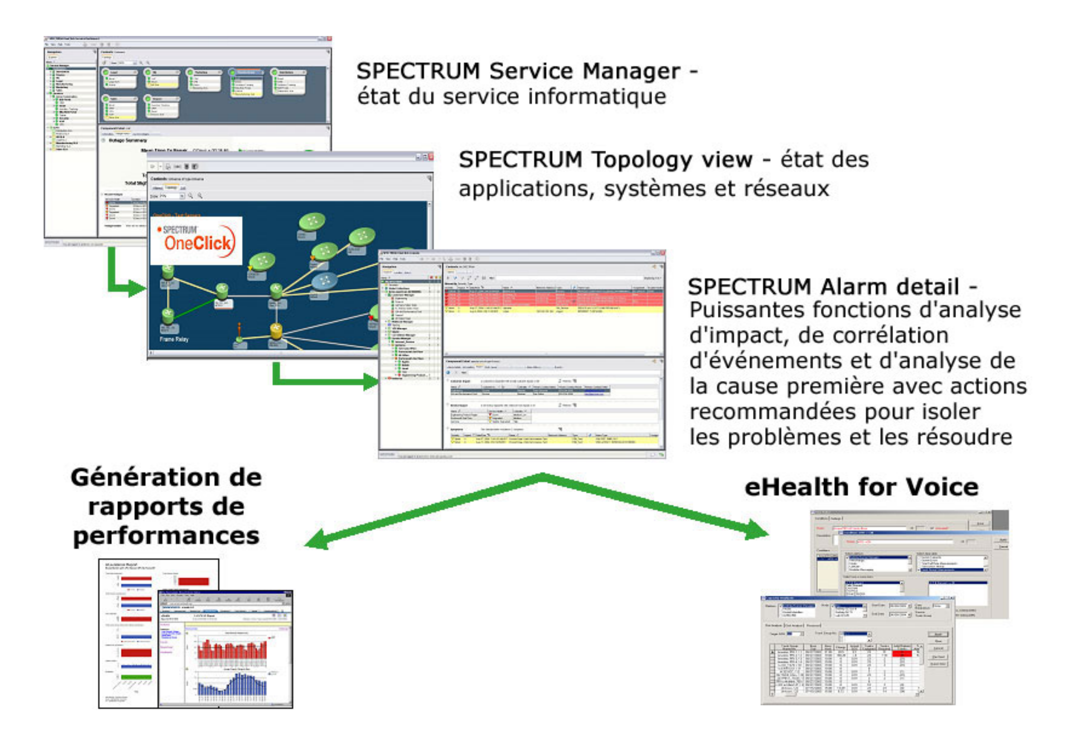
Au sein d'*e*Health, ceci est effectué principalement par le biais des algorithmes Time over Threshold et Deviation from Normal dans Live Health, ce qui permet l'envoi d'une alerte intelligente lorsque les performances actuelles franchissent un seuil fixe ou le comportement considéré comme « normal » (selon l'historique) pendant une durée spécifique dans une fenêtre d'analyse donnée. De même *e*Health for Voice envoie des alertes lorsque la qualité de service ou celle d'écoulement du trafic est insuffisante. Ces alertes sont envoyées dans SPECTRUM, qui applique ses fonctions intelligentes aux stratégies, aux règles et aux modèles de manière à identifier la gravité du problème et à proposer l'intégration et la corrélation des alarmes, tout en tirant parti de SPECTRUM Service Management et de la capacité de modélisation de la voix.



Résolution rapide des problèmes

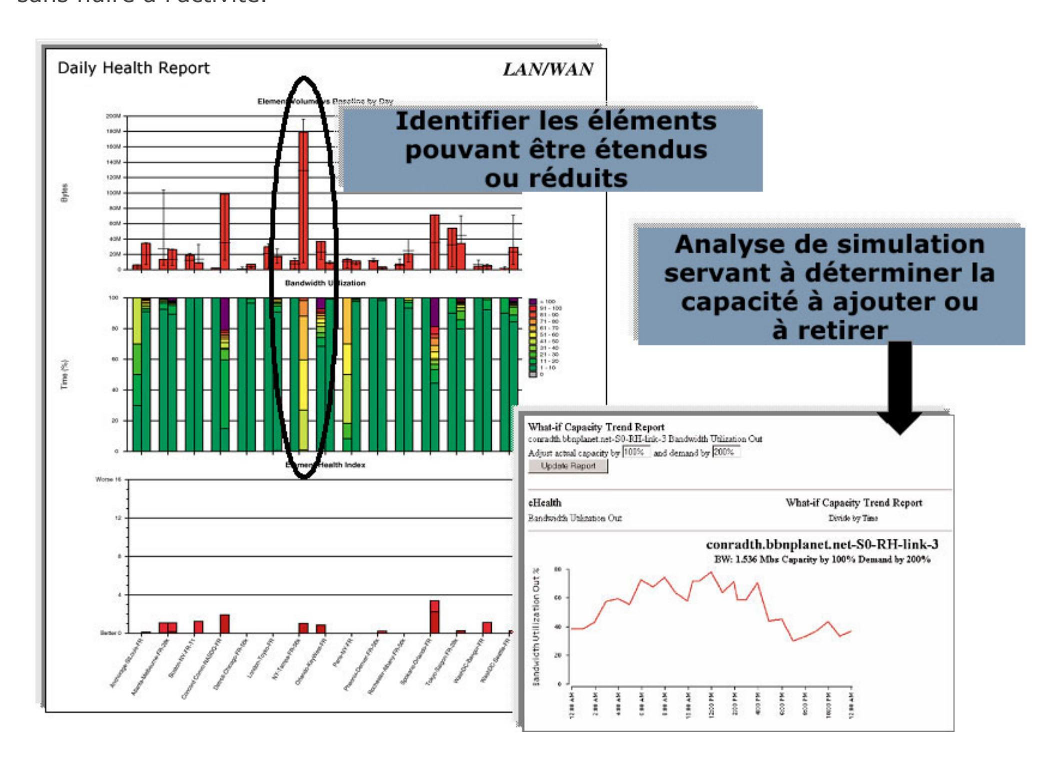
Les produits de gestion des réseaux et de la voix fonctionnent ensemble pour aider les équipes chargées d'exploiter les réseaux à identifier les problèmes relatifs aux infrastructures de voix et de données et à les résoudre rapidement. Les équipes chargées de l'exploitation sont d'abord averties d'un problème potentiel par SPECTRUM Service Manager. Il affiche les services vitaux et modifie leur couleur selon les stratégies établies dans SPECTRUM. Les membres des équipes chargées de l'exploitation peuvent rapidement identifier sur la carte de topologie réseau les périphériques défaillants dans l'infrastructure et effectuer un zoom avant sur les détails des alarmes (y compris celles envoyées par *e*Health ou *e*Health for Voice) dans le rapport Alarm Detail afin de comprendre le problème spécifique. Ils peuvent également accéder aux informations concernant la cause probable dans SPECTRUM, puis lancer *e*Health ou *e*Health for Voice pour obtenir d'autres informations historiques sur les performances et identifier le problème précédent rencontré par le périphérique.



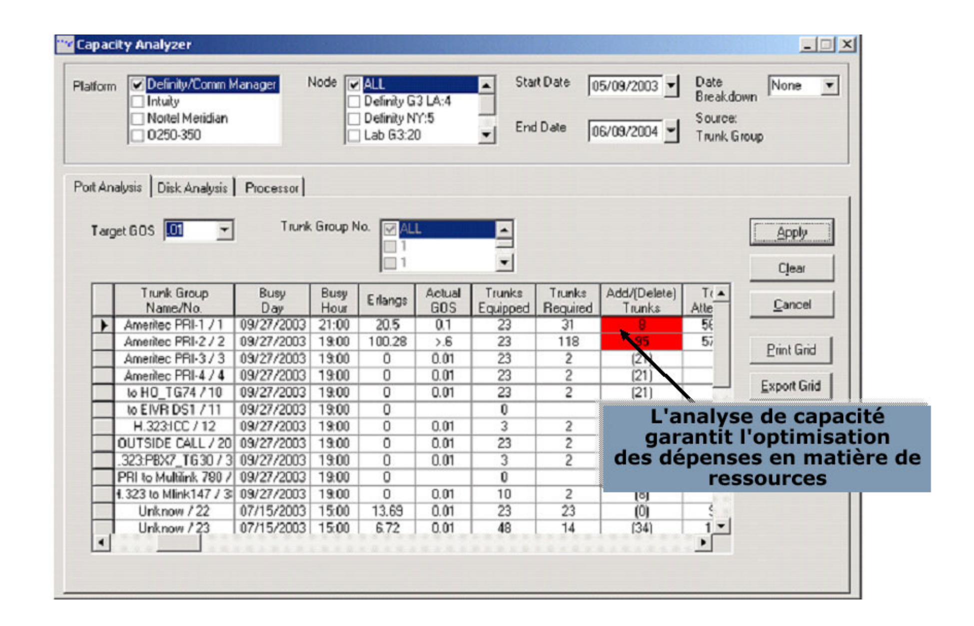


Planification prédictive de la capacité

Les équipes chargées d'exploiter les réseaux utilisent les algorithmes intelligents d'*e*Health et d'*e*Health for Voice afin de déterminer les besoins en capacité nécessaires pour remplir les objectifs validés en matière de qualité du service et de l'écoulement du trafic. Les produits sont également utilisés pour résoudre le problème inverse : déterminer les domaines dans lesquels l'entreprise peut économiser de l'argent en réduisant la capacité sans nuire à l'activité.






Capacity Analyzer
Platform
Definity/Comm Manager
Intuity
Nortel Meridian
O250-350
Node
ALL
Definity G3 LA:4
Definity NY:5
Lab G3:20
Start Date
05/09/2003
End Date
06/09/2004
Date Breakdown
None
Source:
Trunk Group
Port Analysis
Disk Analysis
Processor
Target GOS
.01
Trunk Group No.
ALL
Apply
Clear
Cancel
Print Grid
Export Grid
Trunk Group Name/No.
Busy Day
Busy Hour
Erlangs
Actual GOS
Trunks Equipped
Trunks Required
Add/(Delete) Trunks
Ameritec PRI-1 / 1
Ameritec PRI-2 / 2
Ameritec PRI-3 / 3
Ameritec PRI-4 / 4
to HQ_TG74 / 10
to EIVR DS1 / 11
H.323ICC / 12
OUTSIDE CALL / 20
Unknow / 22
Unknow / 23
L'analyse de capacité garantit l'optimisation des dépenses en matière de ressources


ca

Chapitre 4 : Déploiement de l'architecture de gestion des réseaux et de la voix

Ce chapitre décrit la préparation à l'installation et à la configuration de la solution de gestion des réseaux et de la voix de CA. Il présente les principales rubriques suivantes :

- Composants de 'Performances réseau'
- Composants de 'Gestion des défaillances réseau'
- Composants de 'Gestion de la voix'
- Architectures de déploiement
- Recommandations sur la taille

Composants de 'Performances réseau'

*e*Health est constitué des composants suivants :

Composants obligatoires	Composants facultatifs
E2E Console	Live Health
	Modules d'intégration
	Distributed *e*Health
	Remote Poller
	Report Center
	Traffic Accountant

E2E Console

Le composant E2E Console est au coeur d'une implémentation d'*e*Health. Il est nécessaire au fonctionnement d'eHealth. Il comprend une base de données, une découverte et une fonction d'interrogateur, ainsi que des interfaces graphiques utilisateur d'administration, de génération de rapports, etc. Les licences *e*Health (universelle et système) permettent à la console *e*Health de rechercher des données dans des périphériques certifiés et de les collecter avec un agent de logiciel de gestion intégré. Elles sont nécessaires au fonctionnement d'*e*Health. Un élément représente le modèle *e*Health, ou sa représentation, pour une partie d'une infrastructure pouvant être analysée par *e*Health. *e*Health peut analyser un élément physique, par exemple un port sur la carte d'un routeur. Il peut également analyser un élément logique, qui correspond à la fonction logique d'un périphérique ou d'un composant, tel qu'un lien de réseau. Pour déterminer si un périphérique peut être utilisé avec *e*Health, connectez-vous aux pages de certification à l'adresse http://support.concord.com.



Remarque : Pour accéder au site http://support.concord.com, vous devez posséder un compte d'assistance. Un compte vous est attribué à l'achat des produits *e*Health ou SPECTRUM.

Live Health

Live Health est le moteur de surveillance des performances en temps réel qui analyse les données de performances collectées avec *e*Health en cas d'écart par rapport à la normale et de dépassement de seuil. Live Health comprend trois composants :

- Live Exceptions vous permet de générer des alarmes en fonction des performances et de les afficher.
- Live Status offre une vue unique de bout en bout de l'état de votre infrastructure.
- Live Trend permet de générer des rapports en temps réel.

Modules d'intégration

*e*Health offre un ensemble de modules d'intégration (IM, Integration module) permettant de générer des rapports sur les données collectées par différents systèmes de gestion du réseau. Lorsque vous enregistrez un IM et l'installez, celui-ci vous permet d'accéder aux données déjà collectées par un système de gestion du réseau existant. Vous pouvez alors les importer « en masse » dans *e*Health et obtenir rapidement des données vitales. Ainsi, vous n'aurez plus besoin de collecter des données redondantes via une interrogation dupliquée.

- Les **modules d'intégration Universal Workflow** permettent aux clients de passer des systèmes de gestion des défaillances pris en charge à *e*Health. Ce type d'IM est pris en charge sur les systèmes suivants : SPECTRUM, IBM (Micromuse) Netcool, Cisco Information Center (CIC) et HP OpenView Network Node Manager.
- Les **modules d'intégration Universal Data** permettent l'importation des données de configuration et de performances. Ce type d'IM est pris en charge sur les systèmes suivants : Cisco WAN Manager, Cisco ISC, Lucent, Alcatel et Nortel.
- Les **modules d'intégration Universal Wireless Data** permettent l'importation des données de configuration et de performances depuis d'autres systèmes de gestion d'éléments sans fil dans *e*Health E2E Console. Ce type d'IM est pris en charge sur les systèmes suivants : Nortel Shasta SCS GGSN et Starent ST-16 Bulk Stats.

Distributed eHealth

Dans une infrastructure étendue, vous pouvez déployer plusieurs systèmes Distributed *e*Health sur plusieurs emplacements physiques ou les placer alternativement dans une configuration centrale appelée cluster. Le cluster contient plusieurs systèmes *e*Health qui gèrent des ensembles spécifiques de ressources et partagent des informations. L'utilisation de Distributed *e*Health vous permet de répartir la charge de travail de collecte et de traitement des données sur plusieurs systèmes *e*Health qui fonctionnent en parallèle. Les utilisateurs concernés peuvent accéder aux rapports de tous les éléments ou groupes du cluster depuis les consoles Distributed *e*Health, qui rendent compte des frontaux au cluster.



Vous choisissez généralement un site Distributed *e*Health lorsque vous souhaitez exécuter des rapports pour un nombre d'éléments supérieur à celui qu'un système *e*Health autonome peut prendre en charge. Vous pouvez également choisir un site Distributed *e*Health si vous souhaitez placer un système de serveur Web *e*Health à l'extérieur du pare-feu et isoler les systèmes Distributed *e*Health protégés par le pare-feu de votre infrastructure. En fonction du nombre de systèmes Distributed *e*Health et des performances de la console correspondante, un site Distributed *e*Health peut prendre en charge les rapports d'un million d'éléments.

Le logiciel Package Distributed *e*Health contient tous les logiciels des consoles associées ainsi que celui requis pour transformer un système *e*Health autonome en système réparti. Vous devez acheter séparément tous les logiciels, les éléments et les agents de console pour les systèmes autonomes *e*Health. Pour obtenir des instructions détaillées sur l'administration d'un cluster, consultez le manuel *Distributed* e*Health Administration Guide*.

Remote Poller

Si vous administrez un environnement de grande taille ou étendu, un système *e*Health peut s'avérer insuffisant pour surveiller l'ensemble de vos ressources. L'interrogation à distance vous permet d'installer *e*Health sur des systèmes distants (appelés sites distants) et de configurer chaque site pour interroger un ensemble d'éléments. La base de données sur chaque site *e*Health distant contient les données des éléments interrogés et *e*Health permet de gérer ces éléments sur chaque site. Un système *e*Health central extrait périodiquement les informations sur les éléments et les données de performances depuis les systèmes *e*Health distants et les fusionne dans une base de données *e*Health centrale. Vous pouvez exécuter les rapports de tous les éléments à partir de cette base de données.

Vous choisissez généralement un site d'interrogation à distance lorsque les systèmes d'interrogation doivent se connaître ou partager des informations. Par exemple, les sites distants peuvent gérer des clients distincts d'un fournisseur de services ou des unités d'exploitation distinctes au sein d'une grande entreprise. Il peut s'agir de sites dispersés sur le plan géographique ou de sites locaux séparés par des pare-feux ou d'autres obstacles retardant ou empêchant l'interrogation. Pour obtenir des instructions détaillées sur l'administration d'un système distant d'interrogation, consultez le manuel *Using the* e*Health Remote Poller Guide*.

Report Center

*e*Health Report Center est une application facultative de génération de rapports disponible avec *e*Health r 6.0 et les versions ultérieures. Elle offre une alternative à *e*Health Report Developer Language (RDL), qui permet de personnaliser les rapports *e*Health standard. Report Center permet aux utilisateurs de créer de nouveaux types de rapports *e*Health et de les personnaliser entièrement. Ces rapports peuvent répondre à différents types de questions sur les performances du réseau, du système et des ressources d'application.

Report Center offre une grande flexibilité de personnalisation ainsi que de nombreuses capacités qui permettent aux utilisateurs de modifier l'apparence des rapports et la représentation des données *e*Health existantes. Cette application propose une interface Web, dans le style des dossiers Windows, que les utilisateurs peuvent modifier selon leurs préférences. Cette interface intuitive permet d'identifier, d'afficher et d'exécuter rapidement des rapports. Report Center fournit de précieux exemples de rapports que les utilisateurs peuvent exécuter pour afficher les performances de leurs ressources ou utiliser comme modèles lors de la création de rapports.



Traffic Accountant

La plupart des entreprises qui ont des stratégies basées sur l'e-business et sur Internet doivent s'assurer que les ressources de leur réseau correspondent bien aux besoins des utilisateurs et aux exigences des applications. Il est important de connaître qui utilise la bande passante et les applications qui sont en train d'être utilisées. Traffic Accountant vous permet de surveiller le trafic du réseau à l'aide de sondes RMON2 aux normes industrielles et de routeurs Cisco NetFlow. Traffic Accountant fournit des fonctions sophistiquées de regroupement et de tri pour créer des rapports concis et simples. Vous pouvez profiter d'un aperçu des tendances et des modèles d'utilisation qui altèrent les performances de votre réseau. Traffic Accountant doit fonctionner sur un système *e*Health dédié. En outre, la surveillance du trafic RMON2 et des performances réseau standard requiert l'utilisation de deux systèmes *e*Health pour garantir des performances optimales d'interrogation et de génération de rapports.

Composants de 'Gestion des défaillances du réseau'

SPECTRUM est constitué des composants suivants :

Composants obligatoires	Composants facultatifs	
Assurance Server	Watch Editor	ATM Circuit Manager
Assurance Server Xsight	SNMP V3	Report Manager
Assurance Server Integrity	Alarm Notification Manager	Multicast Manager
Assurance Server Infinity	Secure Domain Manager	Service Performance Manager
OneClick	Frame Relay Manager	QoS Manager
	Configuration Manager	Service Manager
	VPN Manager	

Assurance Server

Le composant Assurance Server de SPECTRUM se décline en trois versions conçues pour différents types de clients :

- Assurance Server Xsight (pour les entreprises récentes)
- Assurance Server Integrity (pour les entreprises plus importantes)
- Assurance Server Infinity (pour les fournisseurs de services)

ASSURANCE SERVER XSIGHT

Assurance Server Xsight offre les fonctionnalités des principales technologies SPECTRUM à un plus vaste éventail de petites entreprises. Grâce à l'introduction de SPECTRUM Xsight, CA a étendu la prise en charge de la gestion des performances et des défaillances IP multifournisseur dans une solution unique et disponible à un prix compétitif qui vous permet de devenir rapidement fonctionnel. Ce composant prend en charge la plupart des périphériques disponibles actuellement sur les réseaux d'entreprise. Il prend uniquement en charge le déploiement sur un serveur unique ; il interdit tout déploiement réparti.



Assurance Server Xsight offre les fonctionnalités clés suivantes :

- Analyse de la cause première
- Analyse d'impact
- Découverte automatique de réseaux multifournisseur et multitechnologique
- Intégrations standardisées
- Une licence d'administrateur de site (licence avec tolérance de pannes non incluse)

ASSURANCE SERVER INTEGRITY

Les produits SPECTRUM reposent sur la notion de fourniture de services à des grandes entreprises dont les activités évoluent, fusionnent et augmentent rapidement. La solution SPECTRUM Integrity a transformé les technologies brevetées de CA et les a combinées avec de nouvelles fonctions pour permettre aux entreprises aujourd'hui en pleine évolution de gérer leurs services vitaux aussi bien au niveau local qu'international. Ce composant prend en charge la plupart des périphériques disponibles actuellement sur les réseaux d'entreprise.

Assurance Server Integrity offre les fonctionnalités clés suivantes :

- Analyse de la cause première
- Analyse d'impact
- Découverte automatique de réseaux multifournisseur et multitechnologique
- Intégrations standardisées
- Une licence d'administrateur de site et une licence avec tolérance de pannes

ASSURANCE SERVER INFINITY

SPECTRUM Infinity se concentre tout particulièrement sur les besoins des fournisseurs de services actuels. Il offre des fonctionnalités spécifiques avec une optimisation sensible des performances visant à accélérer les nouveaux déploiements de services et à dépasser les attentes des clients en matière de qualité, tout en leur permettant de gérer une infrastructure croissante avec les ressources existantes. Ce composant prend en charge Integrity et les unités sophistiquées, généralement présentes uniquement sur les réseaux des fournisseurs de services, grâce au pack Advanced Management Module.

Assurance Server Infinity offre les fonctionnalités clés suivantes :

- Analyse de la cause première
- Analyse d'impact
- Découverte automatique de réseaux multifournisseur et multitechnologie
- Intégrations standardisées
- Une licence d'administrateur de site, une licence avec tolérance de pannes et deux licences d'intégration Southbound Gateway



OneClick

SPECTRUM OneClick est une console Web à trois niveaux. Le composant central est un serveur Web qui se connecte directement aux modules SPECTRUM Assurance Server et qui fournit des informations aux clients Java répartis. Les clients Java, dotés de très nombreuses fonctions, sont téléchargés, installés et mis à jour à partir du serveur Web OneClick pour faciliter l'implémentation, l'administration et la maintenance. Vous pouvez accéder à la console SPECTRUM OneClick à tout moment et en tout point. Celle-ci offre un niveau de modularité et de réactivité équivalent à celui d'une application PC cliente complète, tout en réduisant le temps de formation normalement nécessaire pour se familiariser avec des applications Web standard.

La console OneClick offre les fonctionnalités clés suivantes :

- Console d'événements
- Interface Web intuitive à partir de rôles
- Cartes de topologie complètes
- Configurabilité exceptionnelle de la console d'alarme
- Suite complète d'outils de dépannage
- Sécurité d'administration
- Installation client automatisée
- Licence d'utilisation simultanée

Watch Editor

SPECTRUM Watch Editor permet de surveiller facilement les indicateurs clés de performance sur les infrastructures de réseau, système et d'applications. Il sert également à personnaliser et à augmenter la surveillance. L'ajout de fonctionnalités supplémentaires à SPECTRUM (interrogation, journalisation et définition de seuil) permet d'automatiser la notification et de lancer des scripts lorsque les performances sont modifiées ou en dehors de la plage de référence normale.

Les observations servent à surveiller les statistiques, les calculs complexes et/ou les valeurs qui doivent rester statiques. Les observations peuvent également être configurées et appliquées simultanément à des milliers de périphériques. Les clients utilisent souvent SPECTRUM Watch Editor pour surveiller l'unité centrale, la mémoire, le stockage et l'utilisation de la bande passante selon plusieurs fournisseurs et technologies. La combinaison de ces fonctionnalités constitue un moyen rentable d'observer intelligemment les seuils et d'automatiser les actions correctives de façon proactive sans recourir à des techniques de programmation complexes.

Watch Editor offre les fonctionnalités clés suivantes :

- Création simple de seuils proactifs pour les indicateurs clés de performance relatifs aux infrastructures de réseau, système et d'application
- Automatisation des actions correctives
- Activation des observations en fonction de temporisateurs, d'interrogations, de statistiques et de valeurs calculées



Alarm Notification Manager

SPECTRUM Alarm Notification Manager (SANM) améliore les capacités de traitement des alarmes de SPECTRUM. L'administrateur de stratégies SANM vous permet de spécifier les types d'alarmes à recevoir et d'éliminer les alarmes sans importance. L'interface utilisateur par pointer-cliquer de SANM sert également à contrôler le comportement de l'alarme en fonction des paramètres de planification horaires, quotidiens, hebdomadaires ou mensuels. Les grandes entreprises et les fournisseurs de services exploitent généralement SANM dans des centres d'exploitation réseau contrôlés à distance. En fonction de leurs horaires de travail, des membres spécifiques du personnel informatique peuvent être avertis par SPECTRUM en cas de problème, où qu'ils se trouvent. Ils disposent ainsi facilement d'informations sur la cause première. SANM adapte le texte des alarmes à la catégorie professionnelle concernée : il utilise des termes métier pour communiquer des alarmes aux cadres et des termes techniques pour le personnel informatique. Ce composant constitue un moyen rentable de gérer vos stratégies de notification d'alarme dans votre environnement SPECTRUM.

Alarm Notification Manager offre les fonctionnalités clés suivantes :

- Consolidation d'alarmes
- Filtrage d'alarmes
- Transfert d'alarmes à partir de stratégies
- Notification d'alarmes

Frame Relay Manager

SPECTRUM Frame Relay Manager permet une surveillance étroite et fournit des seuils de performances pour les débits minimaux garantis, l'utilisation de la bande passante et l'encombrement du circuit. Le DLCI (data link connection identifier, identificateur de connexion de liaison de données) assure l'analyse de la cause première et l'isolement des erreurs, avec une analyse d'impact permettant de définir la priorité des réponses et des actions correctives. Les techniques brevetées de découverte automatique exploitent les informations d'adresse IP distante et les statistiques de trafic en fonction de la connectivité DLCI et présentent une vue de la topologie intégrée. Plusieurs grandes entreprises utilisent SPECTRUM Frame Relay Manager pour documenter les violations du contrat de niveau de service avec leurs fournisseurs de services.

SPECTRUM Frame Relay peut également déterminer si une entreprise a acheté trop ou pas assez de bande passante pour chaque circuit. Cette fonction permet de réduire les frais mensuels de connectivité au réseau étendu de plusieurs milliers, voire de dizaines de milliers, de dollars. Les fournisseurs de services ont utilisé SPECTRUM Frame Relay Manager pour garantir le respect des contrats de niveau de service, améliorer la qualité du service clientèle et fournir des offres de services diversifiées. Dans 97 à 99 % des cas, l'utilisation de ce composant permet à un fournisseur de services d'identifier les problèmes Frame Relay *avant* leurs clients et nous nous efforçons de les résoudre avant que l'activité du client ne soit affectée. Ce composant constitue un moyen rentable d'améliorer la qualité de service, de fournir une visibilité de bout en bout et de réduire les coûts d'exploitation.



Frame Relay Manager offre les fonctionnalités clés suivantes :

- Communication proactive et prise en charge des MIB Frame Relay RFC 1315 ou RFC 2115 avec des extensions de fournisseurs pour Cisco et Nortel
- Modélisation rapide et précise de la connectivité de port DLCI physique et logique avec informations sur l'adresse IP, le masque de sous-réseau et l'adresse IP distante
- Des vues de performances prêtes à l'emploi indiquent le débit garanti, les statistiques d'encombrement et les modifications apportées aux DTE (data terminal equipment, équipement terminal de traitement de données)

ATM Circuit Manager

SPECTRUM ATM Circuit Manager permet une surveillance étroite et fournit des seuils de performances pour le débit ATM, l'utilisation de la bande passante et l'encombrement du circuit. L'analyse de la cause première et l'isolement des erreurs est fournie par VPL (virtual private LAN, réseau local privé virtuel) ou par VCL (virtual channel links, liaisons de canaux privées) avec une analyse d'impact permettant de définir la priorité des réponses et des actions correctives. Les techniques brevetées de découverte automatique exploitent les informations sur l'adresse IP distante et les statistiques de trafic en fonction de la connectivité VPI (virtual path identifier, identificateur de chemin virtuel) ou VCI (virtual channel identifier, identificateur de canal virtuel) et présentent une vue de topologie intégrée. La vue du chemin de circuit ATM affiche la correspondance entre les extrémités de chaque périphérique, interface logique ou port physique traversé.

Les entreprises peuvent également importer une liste de circuits virtuels permanents fournie par leur fournisseur de services pour modéliser avec précision toutes les liaisons de réseau étendu ATM. Plusieurs grandes entreprises utilisent déjà SPECTRUM ATM Circuit Manager pour documenter les violations du contrat de niveau de service avec leur fournisseur de services. En plus de cette fonctionnalité, SPECTRUM ATM peut également déterminer si une entreprise a acheté trop ou pas assez de bande passante pour chaque circuit. Cette fonction permet de réduire les frais mensuels de connectivité au réseau étendu de plusieurs milliers de dollars. Les fournisseurs de services ont utilisé SPECTRUM ATM Circuit Manager pour garantir le respect des contrats de niveaux de service et fournir des offres de services diversifiées. Ce composant constitue un moyen rentable d'améliorer la qualité de service, de fournir une visibilité de bout en bout et de réduire les coûts d'exploitation.

ATM Circuit Manager offre les fonctionnalités clés suivantes :

- Communication proactive avec un équipement ATM qui prend en charge le document RFC 1695 avec des MIB (management information bases, bases d'informations de gestion) privées
- Modélisation rapide et précise de la connectivité de port VPL/VCL physique et logique avec informations sur l'adresse IP, le masque de sous-réseau et l'adresse IP distante
- Vues de performances prêtes à l'emploi indiquant le débit en cellules par seconde et des informations relatives à la qualité de service ATM



Multicast Manager

SPECTRUM Multicast Manager fournit une visibilité multifournisseur dans les sessions réseau de multidiffusion logique, en surveillant de manière proactive les indicateurs clés de performance tout en soulignant l'impact des interruptions d'infrastructure sur les services de multidiffusion. Tous les services de superposition de multidiffusion logique sont automatiquement découverts et modélisés dans SPECTRUM Assurance Server. Les modèles de session de multidiffusion maintiennent la connaissance complète du flux de multidiffusion y compris sa source, l'arborescence de distribution ainsi que ses récepteurs.

SPECTRUM Multicast Manager offre à l'utilisateur une interface conviviale pour la navigation dans la topologie et la surveillance des alarmes. Cela permet de réduire les coûts de formation et d'administration car les utilisateurs ont un accès général aux informations exécutables. Les améliorations apportées à la multidiffusion permettent à l'utilisateur d'afficher la topologie de multidiffusion par groupe et les routeurs, commutateurs et ports associés qui se trouvent dans le groupe de multidiffusion IP. SPECTRUM Multicast Manager surveille également l'intégrité du groupe de multidiffusion. Si une ressource d'un groupe de multidiffusion (source, routeurs, commutateurs, ports) rencontre un problème de fiabilité, SPECTRUM Multicast Manager comprend automatiquement l'impact sur l'ensemble du groupe. Ce composant constitue un moyen rentable de gérer votre infrastructure de multidiffusion comme un service métier.

Multicast Manager offre les fonctionnalités clés suivantes :

- Vue multifournisseur des services IP avec présentation détaillée des éléments qui composent un groupe de multidiffusion
- Interface intuitive pour la navigation dans la topologie de multidiffusion et la surveillance des alarmes de groupes, sources, récepteurs et unités de point de rendez-vous

QOS Manager

SPECTRUM QoS Manager permet aux entreprises et aux fournisseurs de services de vérifier et de valider la configuration et l'efficacité des stratégies QoS et des classes de trafic sur l'ensemble de l'infrastructure informatique. Technology Relationship Mapping (mappage des relations technologiques) et la génération de rapports Web découvrent et documentent l'intégrité et les performances de chaque CoS configurée sur le réseau. Les analyses brevetées SPECTRUM intègrent et automatisent intelligemment la modélisation de vos stratégies QoS et classes de trafic pour fournir des analyses de la cause première et influencer la définition des priorités.

SPECTRUM présente une vision unifiée de votre infrastructure QoS avec un explorateur/navigateur convivial qui vous permet d'accéder aux informations sur les périphériques et les niveaux de ports associées à une classe de trafic. De plus, SPECTRUM permet aux utilisateurs d'afficher chaque comportement configuré ainsi qu'un ensemble complet de statistiques sur la création de stratégies, la mise en forme, la mise en file d'attente et la RED (random early detection, détection précoce aléatoire). Les utilisateurs ont accès aux informations d'alarme exécutables lorsqu'une classe spécifique connaît un fort taux d'abandon de paquets ou une longue file d'attente dans la mémoire tampon.



QoS Manager offre les fonctionnalités clés suivantes :

- Accès aux informations sur les périphériques et les niveaux de ports associées à une classe de trafic spécifique
- Vues de performances prêtes à l'emploi relatives aux statistiques de trafic QoS sur la création de stratégies, la mise en forme, la mise en file d'attente et la RED

VPN Manager

SPECTRUM VPN Manager permet aux entreprises et aux fournisseurs de services de découvrir et de gérer automatiquement les performances et la fiabilité des tunnels VPN de couche 3 entre les différents sites. La notification proactive des problèmes éventuels permet de prendre les actions correctives nécessaires avant que les services vitaux et les clients n'en soient affectés. SPECTRUM VPN Manager découvre de manière dynamique la connectivité physique et logique et vérifie la disponibilité via la surveillance des pulsations ping VRF (virtual routing and forwarding, routage et transfert virtuels). Ce composant constitue un moyen rentable d'assurer une gestion intégrée des défaillances et des performances de votre infrastructure VPN.

VPN Manager offre les fonctionnalités clés suivantes :

- Topologie VPN logique
- Communication proactive avec équipement VPN qui prend en charge les MIB VPN RFC 2547 BGP/MPLS avec des extensions de fournisseurs privés
- Modélisation rapide et précise de la connectivité VPN physique et logique
- Vues de performances prêtes à l'emploi des statistiques individuelles de tunnel et de VPN d'agrégation

SNMPv3

SPECTRUM SNMPv3 permet de sécuriser vos communications liées à la gestion. La solution fournit un moteur de conversion pour les demandes et les réponses SNMP v1 et SNMPv3. La technologie SNMPv3 prend en charge la communication avec le réseau, le système, le stockage, la base de données, l'application et les composants de l'infrastructure de sécurité, la gestion proxy des systèmes traditionnels et les communications entre les gestionnaires. Les clients peuvent utiliser l'ensemble des fonctionnalités d'authentification et de chiffrement SNMPv3 pour sécuriser intégralement le trafic de gestion et la configuration/le contrôle des composants de l'infrastructure informatique.

SPECTRUM SNMPv3 offre les fonctionnalités clés suivantes :

- Protection contre les menaces de sécurité
- Authentification
- Confidentialité
- Confirmation
- Compteurs de grande capacité



Secure Domain Manager

Les réseaux répartis et complexes actuels sont contrôlés par des stratégies de sécurité qui empêchent l'utilisation de protocoles de gestion non sécurisés tels que SNMP (Simple Management Network Protocol) v1 ou ICMP (Internet Control Message Protocol) pour la gestion de ces réseaux. Par exemple, une zone démilitarisée (DMZ) sépare un ensemble d'éléments de l'intranet par l'intermédiaire d'un pare-feu pour des raisons de sécurité. Pourtant, il est nécessaire que les services informatiques prennent en charge les entreprises, les processus et les clients, ce qui implique de pouvoir visualiser l'infrastructure complète. SPECTRUM Secure Domain Manager (SDM) permet aux clients de gérer ces domaines en encapsulant en toute sécurité le trafic SNMP et ICMP via une connexion Secure Socket Layer (SSL). Il suffit d'insérer une simple brèche dans le pare-feu pour obtenir une capacité de gestion étendue sans que cela n'affecte les règles de sécurité en vigueur. Cette solution est entièrement transparente pour l'utilisateur final et toutes les applications clientes, éliminant le besoin d'effectuer des tâches d'administration supplémentaires.

Remarque : Cette fonction n'est pas disponible avec Assurance Server Xsight.

Secure Domain Manager offre les fonctionnalités clés suivantes :

- Connecteurs de domaine sécurisé multiples
- Transfert de trafic SNMP et ICMP
- Trafic encapsulé en toute sécurité via XML/SSL sur le protocole TCP (Transmission Control Protocol, protocole de contrôle de transmission)
- Transparence pour les utilisateurs et les applications clientes

Configuration Manager

La gestion des infrastructures complexes d'aujourd'hui implique la maintenance de centaines, voire de milliers, de périphériques vitaux. La capacité à assurer le suivi de leur configuration et à en vérifier l'exactitude peut devenir cruciale. SPECTRUM Configuration Manager est une application intelligente et intégrée permettant l'automatisation de la gestion des configurations vitales de périphériques, de manière à ce que votre entreprise reste opérationnelle. Celle-ci offre les outils dont vous avez besoin pour capturer, modifier, charger et vérifier les configurations de milliers de périphériques multifournisseurs. Grâce à sa conception unique, SPECTRUM Configuration Manager permet aux utilisateurs d'effectuer l'administration des périphériques sur des fichiers de configuration, des identificateurs d'objets MIB (OID) et des attributs SNMP. Chaque configuration est horodatée et identifiée par le numéro de révision. Vous pouvez modifier des valeurs spécifiques de SPECTRUM telles que la fréquence d'interrogation, le nom de communauté ou la chaîne de sécurité.

SPECTRUM Configuration Manager peut charger rapidement toute configuration stockée sur un seul ou plusieurs périphériques simultanément : en recherchant toutes les modifications, en planifiant des chargements automatiques lors des opérations de maintenance ou en rétablissant les configurations sur leur dernier état de fonctionnement connu. Les comparaisons de configurations planifiées automatiquement fournissent une notification immédiate des changements non autorisés. Ce composant offre une gestion de configuration rentable garantissant la continuité des activités.



Configuration Manager offre les fonctionnalités clés suivantes :

- Capture de configuration
- Modification de configuration
- Chargement et restauration de configuration
- Comparaison et validation de configuration
- Planification automatisée

Report Manager

Facile à installer et à déployer, SPECTRUM Report Manager exploite les données sur la disponibilité, les performances, les ressources et la qualité de service collectées par SPECTRUM. Ces données sont accessibles via Internet ou dans un grand nombre de formats d'exportation. Vous pouvez opter pour une identification proactive et apporter des corrections avant que les services et les clients vitaux ne soient affectés. L'efficacité de l'investissement en capital repose sur l'analyse des disponibilités et des ressources de SPECTRUM Report Manager par fournisseur, famille de produit et type de périphérique. Des études démontrent que des rapports précis d'inventaire des ressources peuvent entraîner une réduction de 30 % des dépenses de capital la première année et 5 à 10 % d'économies par rapport au fonctionnement en cours, puisqu'ils permettent de mieux comprendre l'utilisation des ressources et les opportunités de réaffectation. Les rapports de disponibilité identifient la façon dont les fournisseurs et/ou des produits spécifiques améliorent ou détériorent la qualité des services et garantissent que les décisions d'investissement informatique s'appuient sur des informations factuelles. SPECTRUM Report Manager permet à votre entreprise d'évaluer de manière globale les disponibilités, les performances et la qualité de service de l'infrastructure informatique de bout en bout.

Report Manager offre les fonctionnalités clés suivantes :

- Génération automatique de rapports
- Diffusion automatique de rapports par courrier électronique
- Exportation aux formats Adobe PDF, Microsoft Excel et Word
- Licence utilisateur de site unique

Service Performance Manager

SPECTRUM Service Performance Manager (SPM) offre une approche multifournisseur et multi-agent de la gestion des performances, permettant ainsi de rentabiliser les investissements en matière de gestion du temps de réponse. La découverte et la configuration automatiques et intelligentes des points de vérification des performances au sein de l'infrastructure accélèrent le déploiement et optimisent l'efficacité du workflow. Les capacités de résolution des problèmes en temps réel permettent aux opérateurs d'isoler rapidement la cause de la détérioration des performances, tout en testant et en vérifiant ces dernières après correction.



Du point de vue de l'utilisateur final, une application lente est une application détériorée. SPM permet aux clients de mesurer les performances de manière proactive et de détecter les problèmes de réseau, des systèmes ou des applications en rentabilisant les capacités de mesure du temps de réponse déjà déployées au sein de leur infrastructure. Une fois les corrections appliquées, des tests en temps réel permettent de vérifier l'efficacité des réparations. SPM offre une méthode simple de découverte automatique des hôtes de tests de performances, de notification des dépassements de seuils, de résolution centralisée des problèmes et de collecte de données de performances statistiques à des fins de génération de rapports et d'analyse approfondie. Il en résulte une amélioration des performances et une augmentation de la satisfaction des utilisateurs.

Service Performance Manager offre les fonctionnalités clés suivantes :

- Notification en temps réel des dépassements de seuils en fonction de tests factices et planifiés du temps de réponse
- Analyse des valeurs de référence et des seuils
- Découverte automatique des agents de temps de réponse
- Rentabilisation des investissements existants par le déverrouillage de la valeur des agents de performances actuellement déployés : SLA Cisco IP (SAA & RTTMON), MIB Cisco Ping, MIB Nortel Ping, RFC 2925 (Extreme, Juniper, Riverstone), SystemEDGE, Micromuse (Network Harmoni SLA+)

Service Manager

SPECTRUM Service Manager exploite SPECTRUM Business Service Intelligence pour offrir une gestion historique en temps réel des processus métier, des contrats de niveau de service et des clients. Au lieu de poursuivre la gestion au sein d'un silo technologique vertical spécifique (réseau, systèmes, applications, etc.), SPECTRUM Service Manager permet une gestion en silos multiples horizontale associée à la fiabilité des processus métier.

Cet outil comprend les relations physiques et logiques existant entre la disponibilité et les performances des composants de l'infrastructure informatique et les services et clients vitaux qu'ils doivent prendre en charge. Ces composants informatiques sont mis en corrélation avec des services métier logiques tels que le courrier électronique, l'accès Internet, l'entrée des commandes, les finances, etc.

SPECTRUM Service Manager comble l'écart entre le centre d'exploitation et le centre d'assistance clientèle en mettant en corrélation les problèmes de fiabilité de l'infrastructure avec les services concernés et les clients affectés. Les ressources sont alors allouées en fonction de l'importance des services affectés. Des alarmes en temps réel se déclenchent en cas d'interruption de service ou de violation imminente d'un contrat de niveau de service. Elles indiquent notamment la cause première du problème et permettent une intervention rapide avant que l'entreprise ne soit gravement touchée. Un tableau de bord de service renseigne sur l'état de santé en un coup d'oeil. Les rapports historiques indiquent les performances antérieures et les détails des détériorations et des interruptions, ce qui permet à l'entreprise de trouver des solutions pour améliorer les services au fil du temps.



Service Manager offre les fonctionnalités clés suivantes :

- Gestion proactive des services métier et des contrats de niveau de service
- Tableau de bord intuitif sur l'état des services
- Génération de rapports de niveau de service sur Internet
- Licence de tableau de bord de service simultanée unique
- Gestion des services à partir d'autres outils SPECTRUM Assurance Server

Composants de 'Gestion de la voix'

Le produit *e*Health for Voice comprend les composants suivants :

Composants obligatoires	Composants facultatifs
*e*Health for Voice Licence d'utilisation (par système de messagerie/autocommutateur privé) Licence de noeud (une par système de messagerie/d'appel)	*e*Health for Voice Policy Manager

*e*Health for Voice

*e*Health for Voice est une solution de gestion des performances multifournisseurs, multisystèmes (gestion des appels et messagerie vocale) et multitechnologiques (autocommutateurs privés (MRT) et téléphonie sur IP traditionnels) qui simplifie énormément la gestion des réseaux de voix. *e*Health for Voice élimine la collecte manuelle de données et le besoin d'une forte main-d'oeuvre pour la compilation de rapports et la détermination de la qualité d'écoulement du trafic de la téléphonie. Cela se traduit par une amélioration des performances et de la disponibilité des systèmes de voix, le tout à un coût réduit. De plus, *e*Health for Voice est une solution dépourvue d'agent qui ne requiert l'installation d'aucun logiciel sur les systèmes de voix, ce qui simplifie l'installation et accélère considérablement la rentabilisation.

Vous pouvez exécuter une grande variété de rapports destinés aux imprimeurs, aux destinataires de courriers électroniques ou à un intranet d'entreprise. Grâce à *e*Health for Voice, les informations système précises et à la fois actuelles et historiques sont toujours disponibles à des fins d'élaboration de tendances et d'analyse. Les mesures de performances réelles ne sont pas fournies sous forme d'instantanés de données fragmentés, mais automatiquement transmises à un PC ou à une imprimante et ce, quotidiennement.

L'architecture d'*e*Health for Voice permet une évolutivité maximale grâce à des fonctions de modularisation. Sur de plus petites installations, un serveur unique peut contenir la base de données et le module de collecte des données. Sur des applications plus grandes, des serveurs supplémentaires à différents emplacements peuvent faire office d'agents de collecte des données en téléchargeant les données à partir de clusters vers la base de données centrale. Les données peuvent être collectées selon une planification définie par l'utilisateur, 24/24 heures et 7/7 jours, de manière à être intégralement récupérées avant d'être écrasées. Un nombre quelconque d'ordinateurs clients doit pouvoir accéder à la base de données centrale sur un réseau IP pour avoir accès aux données et aux rapports.



Pour surveiller un autocommutateur privé, un système d'appel ou de messagerie, vous pouvez acheter *e*Health for Voice en commandant la licence d'utilisation correspondante (par exemple, achetez CA *e*Health for Voice – Nortel CS-1000 et Meridian pour surveiller les autocommutateurs privés Nortel), puis commander le nombre de licences de noeud approprié. Chaque système d'appel ou de messagerie surveillé requiert une licence de noeud.

*e*Health for Voice Policy Manager

*e*Health for Voice Policy Manager est un composant à connecter au moteur d'*e*Health for Voice pour surveiller l'activité de toutes les données par rapport aux critères définis par l'utilisateur et envoyer une notification automatique lorsque ces critères sont remplis. Ce module vous permet de définir des seuils et des conditions spécifiques au niveau du noeud, de la plate-forme ou du système et de définir des actions de notification, notamment l'envoi de messages électroniques, de la console et du récepteur d'appels, de traps SNMP à SPECTRUM, à Unicenter NSM ou à des systèmes de surveillance tiers et l'exécution de commandes et de scripts personnalisés. Les conditions sont combinées avec une ou plusieurs actions de réponse afin de créer des stratégies. Le service Policy Manager, exécuté sur un serveur d'applications *e*Health for Voice, surveille ensuite les données chargées dans la base de données par rapport à toutes les stratégies actives et déclenche les actions de stratégies appropriées. Vous pouvez acheter Policy Manager en commandant la licence d'utilisation d'*e*Health for Voice correspondante, puis en commandant le nombre approprié de licences de noeud. Chaque système d'appel ou de messagerie surveillé requiert une licence de noeud.

Architectures de déploiement

La solution de gestion des réseaux et de la voix de CA offre deux déploiements standards :

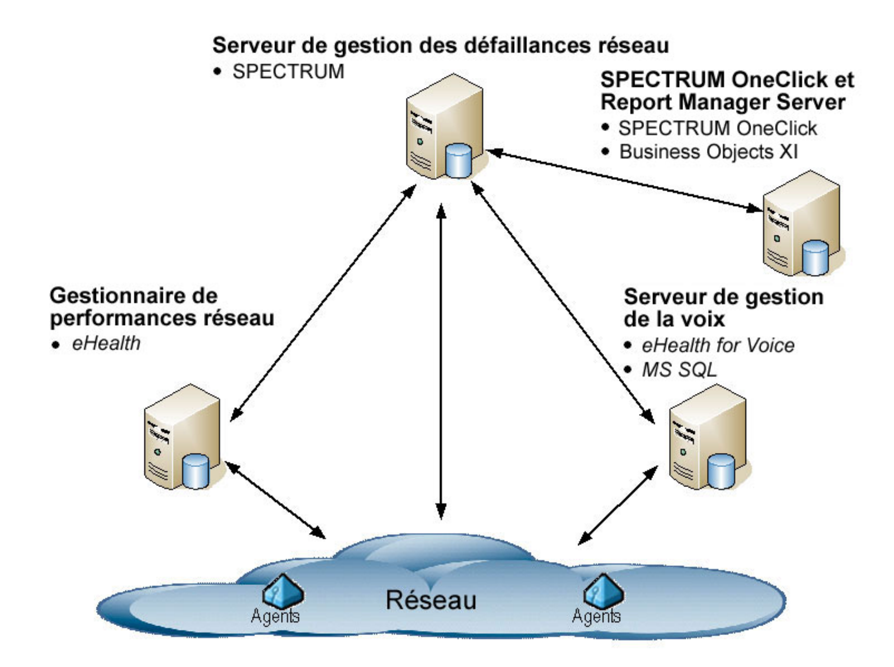
- Petits et moyens déploiements, avec un site de gestion centralisé et un nombre limité de ressources gérées (moins de 100 000) sur une zone géographique restreinte
- Grands déploiements, avec plusieurs sites de gestion répartis possibles, un grand nombre de ressources gérées, éventuellement sur une zone géographique étendue

Les sections ci-dessous illustrent deux exemples de déploiement : le premier déploiement est local, petit à moyen et adapté à une petite entreprise ; l'autre est grand, réparti et prend en charge un fournisseur de services à grande échelle. Les solutions CA peuvent prendre en charge différents déploiements et services métier : plus l'environnement est vaste, plus il est vital de s'appuyer sur CA Technology Services pour planifier, déployer et gérer la solution.

Déploiement dans les petites et moyennes entreprises

En règle générale, un déploiement sur des petites et moyennes entreprises utilise tous les composants de performances décrits dans ce chapitre, à l'exception des produits Distributed *e*Health et Remote Polling. Les utilisateurs possédant au maximum 50 000 ressources gérées, éventuellement sur une superficie limitée, effectuent généralement de petits et moyens déploiements. Le chapitre 5 décrit les recommandations et les procédures de création d'un déploiement à petite ou moyenne échelle. Le graphique ci-dessous représente l'architecture d'un déploiement sur des petites et moyennes entreprises.





Généralement, dans un environnement petit à moyen, vous installez SPECTRUM, *e*Health et *e*Health for Voice sur des systèmes dédiés indépendants. De plus, les applications SPECTRUM OneClick et Report Manager doivent également être installées sur des systèmes dédiés.

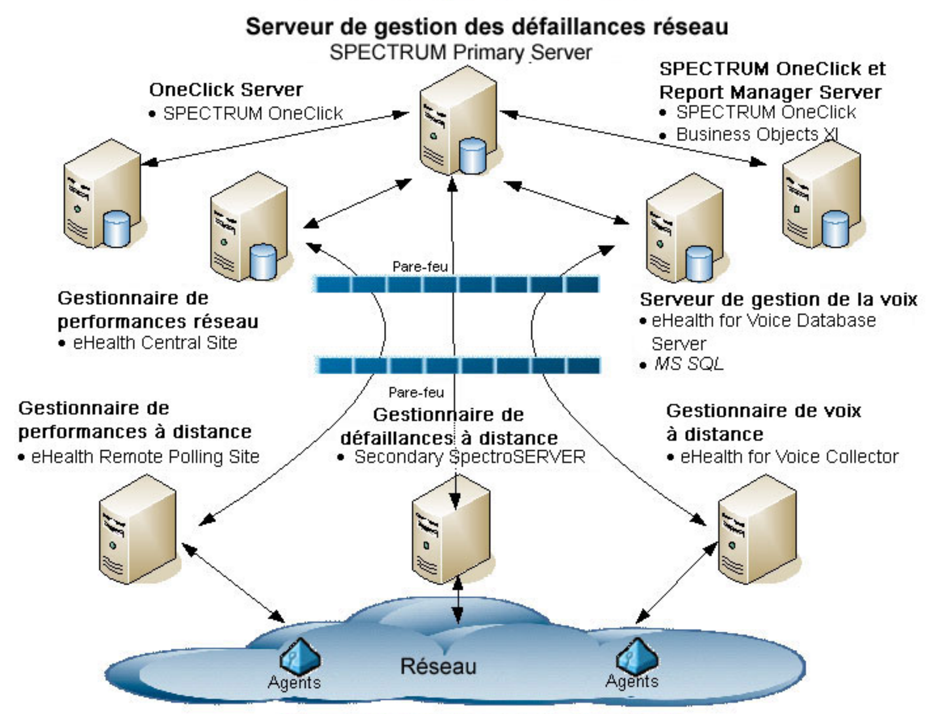
Déploiement chez les grands fournisseurs de services

En règle générale, le déploiement chez un grand fournisseur de services utilise tous les composants, y compris les configurations réparties telles que Distributed *e*Health, *e*Health Remote Polling, Distributed SpectroSERVER et des installations Voice réparties. Les grands déploiements concernent généralement des clients possédant des centaines de milliers de ressources gérées, voire plus, réparties sur une vaste zone géographique. De plus, les fournisseurs de services doivent garantir des vues segmentées des ressources gérées, ces dernières pouvant être « détenues » par des clients indépendants ou leur être allouées.

Ce manuel ne présente pas les procédures de planification et de configuration d'un déploiement à grande échelle. Si vous planifiez une solution de déploiement à grande échelle, renseignez-vous auprès de votre équipe commerciale CA et de CA Technology Services pour planifier et déployer votre configuration en fonction de la taille et des caractéristiques de votre réseau.

Le graphique ci-dessous représente l'architecture d'un déploiement chez un grand fournisseur de services.





La solution de gestion des réseaux et de la voix de CA peut être modulée en fonction de ces configurations. Comme indiqué sur l'illustration, les systèmes centraux sont généralement installés dans la zone du centre d'exploitation du réseau principal. Vous pouvez également installer des systèmes qui collectent les données à partir de zones plus proches des emplacements distants dans lesquels résident les ressources gérées. Les systèmes centraux et distants communiquent afin de partager des informations. La solution CA offre différents moyens de distribuer les services d'interrogation et de couverture de la gestion, ainsi que les services de génération de rapports, de manière à couvrir une large gamme d'environnements de gestion.



Dimensionnement/configuration logicielle et matérielle requise pour les performances réseau

Utilisez l'assistant *e*Health Sizing Wizard afin de déterminer la configuration requise pour l'environnement. Vous pouvez accéder à cet assistant à l'adresse http://www4.concord.com/sizing/swiz. La configuration logicielle et matérielle minimum requise est la suivante :

Spécifications techniques pour *e*Health 6.0 *e*Health E2E Console requise.		
	UNIX	**Windows**
Configuration minimum requise	Serveur Sun ou HP avec UC de 900 MHz minimum	Serveur avec UC de 2 GHz minimum
Systèmes d'exploitation	Solaris 9, 10 (32 et 64 bits)	Windows 2003 : Standard, Enterprise
	HP-UX 11.i, 11.23 (64 bits)	
Windows Manager	OpenWindows, OSF/Motif, CDE	
Mémoire	3 Go	3 Go
Espace d'échange	6 Go	6 Go
Espace disque disponible	14 Go (comprenant les fichiers *e*Health, Oracle, la base de données et l'emplacement de sa sauvegarde)	(Format NTFS) 14 Go (comprenant les fichiers *e*Health, Oracle, la base de données, des applications tierces et l'emplacement de sauvegarde de la BdD)
	Si vous utilisez la fonction Report Center en option, ajoutez 50 % d'espace disque et 1 Go de mémoire.	Si vous utilisez la fonction Report Center en option, ajoutez 50 % d'espace disque et 1 Go de mémoire.
Navigateur Web	Mozilla 1.6 (ou version ultérieure)	Mozilla 1.6 (ou version ultérieure)
		Internet Explorer 6 (ou version ultérieure)
		Mozilla FireFox 1.*x*



Dimensionnement/configuration logicielle et matérielle requise pour la gestion des défaillances réseau

L'utilitaire de dimensionnement SPECTRUM sert à déterminer le nombre de SpectroSERVER nécessaires pour une gestion efficace de votre réseau. Pour plus d'informations sur l'utilisation de l'utilitaire de dimensionnement SPECTRUM, contactez l'assistance technique ou votre représentant CA. La configuration logicielle et matérielle minimum requise est la suivante :

Spécifications techniques pour SPECTRUM 8.0		
	UNIX/Linux	**Windows**
Configuration minimum requise	Sun UltraSPARC II Linux – Pentium Xeon	Pentium Xeon
Systèmes d'exploitation	Solaris 9, 10 (pour plus d'informations sur les correctifs requis, consultez le manuel d'installation)	Windows 2000, Windows XP Professionnel ou Windows 2003 Server
	Linux Red Hat Version 3, mise à jour 6 ou ultérieure	
Mémoire	2 Go	2 Go
Espace disque disponible	40 Go	40 Go

Spécifications techniques pour les serveurs SPECTRUM Report Manager et OneClick		
	UNIX/Linux	**Windows**
Configuration minimum requise	Sun SPARCstation Linux – Pentium Xeon	Pentium Xeon
Systèmes d'exploitation	Solaris 9, 10 (pour plus d'informations sur les correctifs requis, consultez le manuel d'installation)	Windows 2000, Windows XP Professionnel ou Windows 2003 Server Remarque : Business Objects XI prend en charge jusqu'à 10 utilisateurs sur XP.
	Linux Red Hat Version 3, mise à jour 6 ou ultérieure	
Mémoire	1 Go (avec 2 Go d'espace de permutation pour Solaris)	1 Go
Espace disque disponible	4 Go	4 Go
Applications	Mise à jour Linux 6 ou ultérieure Progiciels Solaris SUNWeu8os SUNWeuluf	Pour plus d'informations sur les mises à jour de votre version de Windows, contactez le centre d'assistance Microsoft. Business Objects XI Service Pack 1



Spécifications techniques pour les serveurs SPECTRUM OneClick (sans Report Manager)		
	UNIX/Linux	**Windows**
Configuration minimum requise	Sun SPARCstation Linux – Pentium Xeon	Pentium Xeon
Systèmes d'exploitation	Solaris 9, 10 (pour plus d'informations sur les correctifs requis, consultez le manuel d'installation)	Windows 2000, Windows XP Professionnel ou Windows 2003 Server
	Linux Red Hat Version 3, mise à jour 6 ou ultérieure	
Mémoire	1 Go	1 Go
Espace disque disponible	230 Mo	230 Mo
Applications	Mise à jour Linux 6 ou ultérieure Java 2 SDK, Standard Edition, version 1.5.0_06 ou ultérieure	Windows 2000 - Service Pack 2 ou ultérieur Java 2 SDK, Standard Edition, version 1.5.0_06 ou ultérieure

Configuration logicielle et matérielle requise pour un serveur de base de données ou un PC contenant *e*Health for Voice

	Windows
Configuration minimum requise	Pentium 1GHz ou plus
Systèmes d'exploitation	Windows 2000 Server Windows 2003 Server
Mémoire	512 Mo minimum, 1 Go recommandé
Espace disque disponible	1 Go pour les fichiers programme *e*Health for Voice
	5 à 20 Go pour la base de données en fonction du nombre de plates-formes et de systèmes de voix.
Logiciel de base de données	Microsoft SQL Server 2000 avec Service Pack 2 ou ultérieur ou Microsoft SQL Server 2005 **Remarque :** Le client doit acheter et installer séparément ces logiciels.

Pour connaître la configuration logicielle et matérielle requise pour l'application et des installations sur des clients, reportez-vous au manuel e*Health for Voice Operations Guide.*



Chapitre 5 : Installation et configuration de la solution intégrée

Ce chapitre décrit la procédure d'installation et de configuration des composants de la solution de gestion des réseaux et de la voix de CA **dans un environnement de déploiement petit à moyen**. Il présente également les recommandations relatives à la configuration des composants en vue de la surveillance des performances.

Ce livre vert CA ne décrit pas les procédures de planification et de configuration d'un déploiement à grande échelle. Si vous planifiez une solution de déploiement à grande échelle, renseignez-vous auprès de votre équipe commerciale CA et de CA Technology Services pour planifier et déployer votre configuration en fonction de la taille et des caractéristiques de votre réseau.

Installation des logiciels de la solution de gestion des réseaux et de la voix de CA

Pour créer l'environnement de gestion de la voix et du réseau intégré, vous devez installer les applications SPECTRUM, *e*Health et *e*Health for Voice sur des systèmes dédiés à chaque application.

Important : Les procédures d'installation de chaque application sont décrites en détail dans les manuels d'installation spécifiques aux produits référencés dans ce chapitre. **Vous devez vous référer à ces manuels pour installer correctement les applications.** Reportez-vous d'abord à ce chapitre pour connaître les recommandations de création de la solution intégrée avec ces applications.

Conditions préalables à l'installation

Avant d'aller plus loin, lisez le chapitre 4 du présent manuel pour vous assurer que vos systèmes répondent aux exigences de base et que vous les avez dimensionnés de telle sorte que les applications soient prises en charge dans votre environnement. Si vous ne dimensionnez pas correctement les systèmes, ils ne pourront pas supporter les charges de traitement des applications, ce qui pourrait altérer les performances de la mémoire, de l'espace disque et de l'UC.

Remarque : Votre équipe commerciale CA s'assure que le dimensionnement de vos systèmes tient compte des applications à utiliser et du nombre de ressources à gérer avec ces dernières.

Procédure d'installation

Vous pouvez installer les applications logicielles dans n'importe quel ordre. Il est préférable d'installer d'abord SPECTRUM et SPECTRUM OneClick/Report Manager, puis *e*Health et, enfin, *e*Health for Voice.



Important : Les applications de gestion des réseaux et de la voix de CA exigent que vous utilisiez des systèmes qui leur sont dédiés. N'utilisez **pas** ces systèmes pour d'autres applications ou services. Même si un antivirus et un logiciel de sécurité sont recommandés pour les systèmes du serveur de votre environnement, **désactivez** l'antivirus pendant l'installation pour garantir l'installation complète des applications.

Au moins quatre systèmes sont nécessaires dans la configuration de base suivante :

- SPECTRUM (système SpectroSERVER)
- Serveur SPECTRUM OneClick et Report Manager
- *e*Health
- *e*Health for Voice

RECOMMANDATIONS

Pour faciliter l'installation et la configuration correcte de ces composants, tenez compte des recommandations suivantes :

- Assurez-vous que les systèmes sur lesquels vous comptez installer le logiciel possèdent des adresses IP fixes.
- Obtenez et testez les privilèges du compte de connexion sur les systèmes. Pour les systèmes Windows, vous avez besoin d'un compte disposant des privilèges d'administrateur. Pour les systèmes UNIX, vous devez disposer d'un accès au compte utilisateur racine.

Installation de SPECTRUM

Sur le système désigné comme SpectroSERVER dans votre environnement, installez SPECTRUM version 8.0. Pour obtenir le dernier Service Pack applicable à cette version, connectez-vous au site http://support.concord.com et accédez à la page de téléchargement des logiciels.

Suivez les instructions du manuel *SPECTRUM Installation Guide* pour effectuer les tâches suivantes :

1. Assurez-vous que les conditions préalables de SPECTRUM sont remplies.
2. Préparez le système d'exploitation et optimisez-le afin d'atteindre les meilleures performances.
3. Vérifiez que vous disposez des clés d'extraction et de la licence SPECTRUM. Vous obtenez ces clés auprès du représentant CA lors de l'achat du logiciel.
4. Installez le logiciel et résolvez tous les problèmes éventuels.
5. Démarrez le logiciel SPECTRUM.
6. Activez l'accès au système SPECTRUM.

Après avoir installé SPECTRUM, passez à l'installation de SPECTRUM OneClick.
Installez OneClick de manière à obtenir un accès administrateur complet à SPECTRUM.



Remarque : OneClick est l'interface d'administration principale de SPECTRUM. Utilisez OneClick, plutôt que l'interface traditionnelle SpectroGRAP, pour exécuter les tâches d'administration.

Installation de SPECTRUM OneClick et de Report Manager

Sur le système désigné comme serveur OneClick et Report Manager dans votre environnement, installez SPECTRUM OneClick et Report Manager version 8.0.

Suivez la procédure décrite dans le manuel *Report Manager Installation and Administration Guide* pour exécuter les actions suivantes :

Important : Pour installer les logiciels OneClick et Business Objects suivez attentivement la documentation sous peine de provoquer l'échec de l'installation. Installez d'abord Business Objects et sélectionnez l'option permettant d'utiliser un serveur d'application Java existant. En cas d'échec, vous devez supprimer et réinstaller OneClick et Report Manager.

1. Assurez-vous que les conditions préalables et la configuration requise pour OneClick sont bien respectées.

2. Préparez le système d'exploitation et optimisez ses paramètres afin d'atteindre les meilleures performances.

3. Installez le logiciel et résolvez tous les problèmes éventuels.

4. Installez le client OneClick pour exécuter l'application et vérifiez que vous pouvez vous connecter au système SpectroSERVER.

5. Dans l'interface OneClick, cliquez sur l'onglet Report Manager de la page d'index OneClick pour vérifier que Report Manager est installé correctement.

Installation d'*e*Health

Sur le système désigné comme serveur *e*Health dans votre environnement, installez *e*Health version 6.0. Connectez-vous au site http://support.concord.com et accédez à la page de téléchargement de logiciels pour obtenir le dernier kit InstallPlus de cette version.

Suivez les instructions du manuel *New Installations of* e*Health 6.0 Guide* correspondant à votre plate-forme système (Windows ou UNIX) pour exécuter les actions suivantes :

1. Assurez-vous que les conditions préalables du système sont remplies et vérifiez les emplacements des logiciels *e*Health et Oracle incorporés.

2. Installez les logiciels *e*Health et Oracle et résolvez tous les problèmes éventuels.

3. Vérifiez que vous disposez des licences *e*Health relatives aux fonctions que vous souhaitez utiliser. Vous obtenez ces licences à l'achat des produits *e*Health. Pour *e*Health version 6.0 GA, notez que vous avez besoin d'une licence *e*Health SPECTRUM Integration pour configurer la solution intégrée et l'utiliser.



Important : Une fois l'installation d'*e*Health terminée, suivez les instructions spécifiées dans la section Configuration de la solution intégrée du présent chapitre. **Ne suivez pas** les instructions relatives au démarrage de la console *e*Health et à la découverte des ressources en tant qu'éléments. Vous découvrez les éléments *e*Health de la solution intégrée en important la configuration SPECTRUM à partir du système SpectroSERVER, ce qui simplifie les tâches d'administration relatives à la découverte d'*e*Health.
Pour obtenir une description des tâches d'administration et des interfaces *e*Health, reportez-vous au manuel e*Health Administration Overview Guide*.

Installation d'*e*Health for Voice

Sur le système désigné comme serveur *e*Health for Voice dans votre environnement, installez *e*Health for Voice version 4. Vous pouvez installer *e*Health for Voice dans son intégralité sur un seul PC. Vous pouvez également installer le logiciel dans une configuration répartie sur plusieurs PC, constituée d'un serveur de base de données et de systèmes clients qui peuvent accéder au premier pour les rapports et les tâches d'administration.

Le serveur Database Manager requiert un moteur de base de données Microsoft SQL Server. Vous devez acheter Microsoft SQL Server et l'installer avant *e*Health for Voice. Pour ce faire, il suffit généralement d'installer Microsoft SQL Server 2000 sur le PC qui doit héberger la base de données *e*Health.

Remarque : Microsoft SQL Server est uniquement requis sur le PC qui héberge la base de données *e*Health for Voice (l'installation Database Manager). Il n'est pas nécessaire sur des ordinateurs agents ou clients.

Suivez les instructions du manuel e*Health for Voice Operations Guide* pour exécuter les actions suivantes :

1. Vérifiez que les conditions préalables du système sont remplies.
2. Installez le logiciel et résolvez tous les problèmes éventuels.
3. Si vous le souhaitez, installez les serveurs clients pouvant accéder au serveur de base de données *e*Health for Voice.
4. Démarrez la console de programmation et définissez votre environnement de voix :
   a. Installez les licences des plates-formes à prendre en charge.
   b. Lancez les services suivants (au minimum) :
      - Task Scheduler
      - Data Collector
      - Data Loader
      - Policy Manager
   c. Définissez les éléments suivants :
      - Société
      - Groupe
      - Collecteur
      - Plate-forme
   d. Vérifiez la collecte de données planifiée dans la file d'attente appropriée.



5. Configurez l'intégration SPECTRUM en suivant les instructions du manuel *eHealth for Voice Integration for SPECTRUM Guide*.

Une fois l'installation d'*e*Health for Voice effectuée, suivez les instructions pour démarrer la console de programmation et définir votre environnement de voix. Configurez ensuite l'intégration SPECTRUM conformément aux instructions du manuel *eHealth for Voice Integration for SPECTRUM Guide*.

Configuration de la solution intégrée

A l'aide de SPECTRUM, de SPECTRUM OneClick, d'*e*Health et d'*e*Health for Voice, vous pouvez déployer une solution intégrée pour gérer vos ressources de réseau et de voix.

- SPECTRUM fournit l'interface de gestion principale permettant l'identification des ressources, la gestion des défaillances et la résolution des problèmes du réseau informatique. SPECTRUM réduit les bruits d'alarmes et détecte la cause première des problèmes.
- *e*Health permet la gestion des performances en collectant des statistiques détaillées sur vos ressources et en analysant les données pour détecter l'apparition de problèmes et les modifications du comportement. *e*Health Live Health compare les performances aux seuils et aux règles de service et déclenche des alarmes lorsque les performances des ressources commencent à se détériorer. Les rapports de santé et Live Health peuvent envoyer des alarmes (traps) à SPECTRUM afin que les problèmes apparaissent sur les vues OneClick.
- *e*Health for Voice gère le service de bout en bout pour les réseaux de voix traditionnels, ainsi que pour les réseaux convergents Voice sur IP. Il peut détecter les violations de stratégies de service et les problèmes de capacité et envoyer des alarmes à SPECTRUM pour prévenir les gestionnaires réseau par le biais des vues OneClick.

Même si ces produits peuvent être utilisés séparément pour gérer les performances et les défaillances du réseau et pour générer des rapports sur ces éléments, leurs fonctions combinées offrent aux gestionnaires réseau une vue principale unique des problèmes éventuels et des modifications apportées aux performances du réseau. Ces produits permettent également d'effectuer un zoom avant sur les rapports pour obtenir des informations plus détaillées et pour résoudre les problèmes.

Recommandations

Les sections suivantes décrivent les recommandations de configuration de la solution intégrée de gestion des réseaux et de la voix de CA. Ces recommandations rationalisent les tâches d'administration ordinaires et réduisent le temps dédié à la gestion et à la maintenance des configurations logicielles.

Pour configurer la solution intégrée, suivez la procédure générale ci-dessous :

1. Identifiez les ressources réseau à gérer à l'aide de SPECTRUM Discovery, puis créez des collections globales pour organiser ces ressources.

2. Importez les ressources découvertes avec SPECTRUM dans *e*Health à l'aide du processus de découverte d'*e*Health.



3. Facilitez la génération de rapports et la gestion de vos ressources en organisant les éléments correspondants en groupes et en listes de groupes en fonction de relations telles que la zone géographique, le client, l'entreprise ou le service pris en charge.

4. Planifiez les découvertes *e*Health de collections globales pour conserver la configuration de l'interrogateur.

Les sections suivantes décrivent cette procédure plus en détails et fournissent des références sur la documentation complète relative aux produits.

Identification des ressources et utilisation de SPECTRUM pour les découvrir comme des collections globales

Utilisez SPECTRUM Discovery pour identifier les ressources réseau à gérer, puis créez des collections globales afin d'organiser ces ressources dans les vues de topologie. Ces vues aident les opérateurs réseau à suivre les différentes collections d'entités réseau, d'entreprises ou de services contenus dans votre infrastructure.

De plus, *e*Health Discovery utilise les collections globales comme entrée. La procédure suivante décrit la création d'une collection statique d'éléments à la volée. SPECTRUM offre de nombreux types de découvertes et d'approches. Pour déterminer l'approche la plus efficace pour votre entreprise, reportez-vous aux manuels *Modeling Your IT Infrastructure Administrator Guide* et *AutoDiscovery User Guide.*

Pour créer une collection :

1. Connectez-vous à la console SPECTRUM OneClick, puis sélectionnez Tools, Utilities, Discovery, New Discovery.

2. Dans la boîte de dialogue Discovery, exécutez les actions suivantes :

   a. Spécifiez un nom de configuration.

   b. Spécifiez une plage ou une liste d'adresses IP ou importez un fichier.

   c. Spécifiez une chaîne de communauté valide.

   d. Sous Modeling Options, sélectionnez Discover Only.

   e. Cliquez sur Discover.

   f. A l'apparition des résultats, identifiez les périphériques que vous ne souhaitez pas surveiller, cliquez avec le bouton droit de la souris et excluez-les.

   g. Sélectionnez Model.

   h. Sélectionnez les options de modélisation souhaitées sous Modeling Options.

   i. Cliquez sur OK.

   j. Cliquez sur Close.

   k. Sélectionnez Yes pour enregistrer la configuration Discovery.

   l. Sélectionnez Cancel pour fermer la boîte de dialogue Discovery.



3. Dans le volet de navigation OneClick, sélectionnez l'onglet Locator et utilisez une option de recherche pour trouver des ressources selon des critères spécifiques (par exemple, l'adresse IP ou le nom du modèle).
4. Sélectionnez un ou plusieurs éléments, puis cliquez avec le bouton droit de la souris pour choisir Add To, Collections.
5. Dans la boîte de dialogue Select Collections, cliquez sur Create.
6. Spécifiez un nom et une description pour la collection, puis cliquez sur OK.
7. Cliquez sur OK.

Pour tenir votre configuration à jour, vous pouvez exécuter ce processus régulièrement.

Importation de collections globales dans *e*Health

Importez les ressources découvertes avec SPECTRUM dans *e*Health à l'aide du processus de découverte d'*e*Health. *e*Health peut alors commencer à interroger les ressources automatiquement et créer ainsi une base de données et un historique des performances. Grâce à cette base de données des performances, les rapports *e*Health et Live Health permettent de détecter les modifications du comportement, d'identifier les problèmes liés à la détérioration ou à la capacité des services et de fournir un aperçu des tendances des performances au fil du temps.

CONFIGURATION DE SPECTRUM INTEGRATION

Avant d'importer des collections globales dans *e*Health, exécutez le programme de configuration de SPECTRUM sur le système *e*Health.

Pour exécuter le programme de configuration d'*e*Health SPECTRUM Integration :

1. Connectez-vous au système *e*Health en tant qu'administrateur *e*Health.
2. Ouvrez une fenêtre de terminal et accédez au répertoire *e*Health en saisissant la commande suivante, où e*health* représente le nom de chemin complet :

   cd e*health*
3. Exécutez le programme de configuration en entrant la commande suivante :

   ./bin/nhSPECTRUMSetup

   La boîte de dialogue SPECTRUM Import Setup s'affiche.
4. A l'invite du programme de configuration, saisissez les informations suivantes :
   - Nom d'hôte ou adresse IP du serveur SPECTRUM OneClick
   - Numéro de port des requêtes Web du serveur OneClick
   - Chemin d'installation de OneClick sur le serveur
   - Nom d'utilisateur utilisé pour la connexion au serveur OneClick
   - Mot de passe associé au nom d'utilisateur spécifié
5. Cliquez sur OK. *e*Health vérifie vos paramètres et renvoie un message indiquant leur validité.

   Remarque : Le processus de validation peut prendre quelques secondes.



DÉCOUVERTE DE COLLECTIONS GLOBALES SPECTRUM

Utilisez le processus de découverte *e*Health pour importer la configuration SPECTRUM dans *e*Health.

Pour découvrir une collection globale SPECTRUM :

1. Connectez-vous à la console *e*Health.
2. Sélectionnez Setup, Discover.
3. Dans la boîte de dialogue Discover, exécutez les actions suivantes :
   a. Dans la liste Mode, sélectionnez les types de technologie associés aux ressources à découvrir.
   b. Sélectionnez SPECTRUM Import et spécifiez la collection globale SPECTRUM à importer.
   c. Cliquez sur Discover.

   *e*Health se connecte au serveur OneClick, extrait les informations de la collection SPECTRUM et découvre les éléments appropriés.
4. Enregistrez les éléments découverts dans la configuration de l'interrogateur. *e*Health commence automatiquement à les interroger pour collecter les données de performances.

Organisation de vos ressources en groupes *e*Health

*e*Health contient une fonction de regroupement qui permet d'organiser vos éléments de manière efficace, de faciliter l'administration et de simplifier la génération de rapports. En ciblant un sous-ensemble d'éléments plutôt que tous les éléments de votre infrastructure, vous pouvez les gérer plus facilement et créer des rapports efficaces répondant à des besoins spécifiques. Pour gérer votre infrastructure, vous pouvez organiser les éléments correspondants en groupes selon les zones géographiques, les clients, les entreprises ou les services qu'ils prennent en charge. Vous pouvez organiser vos groupes en les associant à des listes.

Par exemple, si vous souhaitez surveiller les systèmes prenant en charge vos activités en Europe, vous pouvez créer un groupe nommé Angleterre (composé de ressources qui prennent en charge les bureaux de ce pays), ainsi que d'autres groupes pour chaque pays où vous travaillez. Vous pouvez ensuite ajouter ces groupes à une liste de groupes nommée Europe et générer des rapports pour la liste entière. Pour simplifier la génération de rapports et l'administration, vous pouvez également filtrer vos listes d'éléments selon votre stratégie de regroupement. Avant de grouper vos ressources, reportez-vous aux recommandations de regroupement d'*e*Health décrites dans le manuel e*Health Element and Poller Management Guide*.



Pour créer un groupe :

1. Connectez-vous à la console OneClick for *e*Health en tant qu'administrateur autorisé à gérer des groupes.

2. Dans le dossier Managed Resources, sélectionnez Find Elements.

3. Sélectionnez les éléments à inclure. Pour filtrer la liste, sélectionnez Element Chooser. Ajoutez un caractère générique tel qu'un astérisque (*) pour désigner plusieurs caractères ou un point d'interrogation (?) pour en représenter un seul.

4. Cliquez avec le bouton droit de la souris et sélectionnez Create Group with Selected Elements.

5. Spécifiez le nom du premier groupe et sa description. Si la fonction SmartTree est activée, ajoutez au nom du groupe une étiquette indiquant l'emplacement des éléments et utilisez les délimiteurs sélectionnés (par exemple : Angleterre-1, Allemagne-1 ou Espagne-1).

6. Cliquez sur OK. Le groupe apparaît immédiatement sous By Group.

7. Pour créer d'autres groupes avec un suffixe, répétez les étapes 2 à 6. Par exemple : Angleterre-2, Allemagne-2, Espagne-2.

8. Sous Managed Resources, sélectionnez By Group. Si la fonction SmartTree est activée, l'arborescence des éléments affiche deux niveaux séparés et classés par ordre alphabétique en fonction de cette convention de dénomination.

Pour ajouter les groupes à une liste de groupes :

1. Connectez-vous à la console OneClick for *e*Health en tant qu'administrateur autorisé à gérer des groupes.

2. Dans le dossier Managed Resources, cliquez avec le bouton droit de la souris sur By Group List et sélectionnez New Group List.

3. Spécifiez un nom et une description, puis cliquez sur OK.

4. Sous By Group List, double-cliquez sur le nom de la liste de groupes et sélectionnez l'onglet Groups Not in This Group List.

5. Sélectionnez les groupes à inclure, cliquez avec le bouton droit de la souris et choisissez Add Selected Groups to Group List.

6. Cliquez sur Yes pour valider votre choix.

7. Cliquez sur OK pour enregistrer.

Planification des découvertes *e*Health de collections globales

Pour conserver les définitions des éléments dans la configuration de l'interrogateur, vous pouvez planifier des découvertes *e*Health de collections globales. Un job de découverte planifiée s'exécute automatiquement pour mettre à jour les informations des éléments et garantir que les éléments que vous surveillez répondent toujours aux interrogations d'*e*Health.



Pour planifier un processus de découverte :

1. Connectez-vous à la console *e*Health.

2. Sélectionnez Setup, Schedule Jobs.

3. Dans la liste Add de la boîte de dialogue Schedule Job, sélectionnez Add Discover. (Par défaut, la liste Add est définie sur Add At-a-Glance.)

4. Dans la boîte de dialogue Add Scheduled Discover Job, effectuez toutes les opérations suivantes et cliquez sur Schedule :

    a. Sous Mode, sélectionnez un ou plusieurs types d'éléments.

    b. Sélectionnez SPECTRUM Import et spécifiez la collection globale.

    c. Spécifiez la date et l'heure auxquelles vous souhaitez exécuter le job de découverte planifiée. Il est préférable d'exécuter la découverte planifiée *e*Health après les mises à jour de SPECTRUM AutoDiscovery, de manière à ce que vos configurations restent synchronisées. Si votre environnement évolue peu, planifiez des mises à jour moins fréquentes pour les découvertes. Si votre environnement est très dynamique, planifiez des mises à jour plus fréquentes afin de garantir le maintien à jour de vos informations de configuration.

    d. Cliquez sur Schedule.

    e. Cliquez sur OK.

Surveillance du réseau et de la voix

La solution intégrée de CA vous permet de surveiller de près les performances de vos ressources de réseau et de voix. L'application *e*Health Live Health fournit des informations instantanées sur les points sensibles. Elle vous indique l'emplacement des problèmes, leur date de début, ainsi que leur gravité. Elle identifie également les problèmes croissants avant qu'ils n'engendrent des échecs, vous permettant d'agir et de maintenir un fonctionnement normal de votre activité. Live Exceptions envoie des notifications d'alarmes à l'interface SPECTRUM. Vous pouvez ensuite générer des rapports à partir de l'interface SPECTRUM OneClick afin de consulter l'analyse des problèmes effectuée par *e*Health.

Pour configurer la solution intégrée et surveiller les performances, suivez la procédure générale suivante :

1. Configurez la surveillance Live Health des groupes et listes de groupes *e*Health.

2. Transférez les traps Live Health à SPECTRUM.

3. Personnalisez et planifiez les rapports *e*Health pour envoyer des traps à SPECTRUM.

4. Configurez *e*Health for Voice pour envoyer des alertes à SPECTRUM.

5. Configurez SPECTRUM pour reconnaître le serveur *e*Health.

6. Configurez SPECTRUM pour afficher les alarmes d'*e*Health.

Les sections suivantes décrivent cette procédure plus en détail et renvoient à la documentation produit pour des informations complètes.



Configuration de Live Health

Une fois les ressources à surveiller découvertes et groupées, vous pouvez les associer à un profil Live Health pour indiquer le moment où les problèmes de performances se produisent. Un profil Live Health est un ensemble de règles d'alarmes appliquées par *e*Health aux groupes ou aux listes de groupes d'éléments. Les règles d'alarmes définissent les types d'éléments et les conditions à surveiller, les seuils et la durée des problèmes, ainsi que leur gravité.

*e*Health offre des centaines de profils techniques permettant de gérer vos ressources réseau. Pour chaque technologie, *e*Health propose les types de profils Live Health suivants :

Nom du profil	Description de l'objectif
Echec	Identifie les problèmes de disponibilité, les erreurs ou autres échecs de périphériques.
Retard	Signale la présence de problèmes d'encombrement ou de surexploitation pouvant entraîner des retards sur le réseau.
Charge de travail inhabituelle	Indique les moments où la capacité ou le volume d'un élément dépasse ses performances de base habituelles.
Latence	Identifie les ralentissements du réseau. La latence est généralement mesurée entre le système *e*Health et le périphérique lui-même.
Changement de configuration	Détecte les modifications apportées à la configuration d'un périphérique, telles que les insertions de cartes/modules dans un commutateur.
Sécurité	Signale les problèmes tels que la détection d'une attaque « ping of death » par le pare-feu, les échecs de connexion ou les accès non autorisés.

Lorsque vous affectez un profil à un groupe ou à une liste de groupes d'éléments, Live Exceptions surveille le groupe ou la liste à la recherche de toute activité contraire aux règles spécifiées et génère des alarmes lorsque l'activité déclenche une règle dans le profil. Grâce à cette solution intégrée, vous pouvez configurer Live Health de manière à envoyer des alertes à l'interface SPECTRUM en cas de problème. Consultez attentivement l'aide en ligne Live Exceptions disponible avec le produit pour vous assurer d'avoir compris les différents types de performances et la façon dont les règles identifient les problèmes de performances.

RECHERCHE DE PROFILS LIVE EXCEPTIONS

La fonction Live Exceptions comporte des centaines de profils par défaut qui peuvent servir à surveiller les ressources. Pour rechercher et consulter les profils qui s'appliquent à vos types de ressources, utilisez l'outil Live Health Profiles du site d'assistance *e*Health Certification.



Pour consulter les profils Live Exceptions disponibles :

1. Connectez-vous au site http://support.concord.com à l'aide d'un navigateur Web.

2. Cliquez sur Certification.

3. Sur la page Certification, sous Certification Information, cliquez sur Live Health Profile Descriptions.

4. Cliquez sur Element Types pour afficher les différents types de ressources qu'*e*Health peut surveiller.

5. Dans la liste d'éléments, recherchez les types actuellement surveillés. Par exemple, si vous surveillez des UC, cliquez sur CPU, Router/Switch CPU (1) et Generic Router/Switch CPU (2).

6. Cliquez sur un nom de profil et consultez sa description pour déterminer les types de problèmes pour lesquels des alarmes seront déclenchées.

Vous pouvez également créer des profils et des règles personnalisés. Pour savoir comment créer des règles et des profils, reportez-vous à l'aide en ligne Live Exceptions.

DÉMARRAGE DE LIVE EXCEPTIONS ET ASSOCIATION DE PROFILS

Pour utiliser Live Exceptions, vous devez vous connecter à l'interface Web *e*Health et télécharger l'application cliente Live Health sur votre ordinateur ou station de travail local(e). Installez le client Live Exceptions en suivant les instructions fournies sur la page de téléchargement.

Pour accéder à l'interface Web *e*Health, utilisez un navigateur Web pour atteindre la page http://*hostname*:*port*, où *hostname* représente le nom ou l'adresse IP du système *e*Health et *port* correspond au port HTTP utilisé par le serveur Web. Si votre serveur Web utilise le port 80 par défaut, vous pouvez omettre le numéro de port. Pour vous connecter à l'interface Web *e*Health, vous devez posséder un compte utilisateur Web *e*Health.

Pour configurer Live Health et générer des alarmes en cas de problème :

1. Vérifiez que le logiciel client Live Health a été téléchargé et installé à partir de l'interface Web *e*Health.

2. Pour ouvrir l'application Live Exceptions, effectuez l'une des opérations suivantes :

    - Si vous utilisez un système Windows, sélectionnez Démarrer, Programmes, *e*Health, Live Exceptions. Le nom du groupe de programmes varie en fonction du nom utilisé lors de l'installation du client Live Health.
    - Sur un système UNIX, accédez au répertoire d'installation du client Live Health et exécutez la commande nhLiveExceptions.

3. Dans le champ *e*Health System de la fenêtre d'application Live Exceptions, spécifiez le nom du système auquel vous souhaitez vous connecter, ainsi que votre nom d'utilisateur et mot de passe. Le navigateur Live Exceptions s'affiche.

4. Sélectionnez Setup, Subjects to Monitor.

5. Dans la boîte de dialogue Setup Subjects, cliquez sur New.



6. Dans la boîte de dialogue Setup Subjects Editor, associez un profil à un groupe ou à une liste de groupes.

   a. Dans la liste Subjects, sélectionnez un groupe ou une liste de groupes d'éléments à surveiller à l'aide de Live Health.

   b. Sélectionnez un profil approprié dans la liste correspondant au type d'éléments contenu dans le groupe ou la liste de groupes.

   c. Sous Calendars, sélectionnez un calendrier pour spécifier la plage horaire pendant laquelle Live Health doit appliquer le profil au groupe ou à la liste de groupes.

   d. Cliquez sur OK.

   e. Cliquez sur OK pour valider votre sélection, puis sur OK dans la boîte de dialogue Setup Subjects. Cliquez ensuite sur OK pour confirmer l'envoi des modifications au serveur *e*Health.

   Live Exceptions commence à surveiller le groupe ou la liste de groupes afin d'identifier toute activité contraire aux règles spécifiées. Lorsque l'activité déclenche une règle du profil, Live Exceptions active une alarme. En règle générale, les alarmes apparaissent 15 à 20 minutes après plusieurs interrogations d'éléments consécutives.

Transfert de traps Live Health à SPECTRUM

En transférant des traps d'*e*Health Live Health vers SPECTRUM, vous pouvez gérer les alarmes Live Exceptions depuis la console SPECTRUM OneClick, afficher les rapports sur les détails de l'alarme et effacer des alarmes pour réduire le délai moyen de réparation en cas de problème réseau.

Pour configurer Live Exceptions et transférer des traps :

1. Lancez le navigateur Live Exceptions.

2. Sélectionnez Setup, Trap Destinations.

3. Dans la boîte de dialogue Trap Destinations Manager, cliquez sur New.

4. Sous Edit Trap Destination, spécifiez les informations ci-dessous pour le SpectroSERVER :

   › Nom de l'hôte
   › Adresse IP
   › Numéro de port

5. Cliquez sur Add.

6. Vérifiez l'apparition du nom du SpectroSERVER dans la liste Existing Trap Destinations, puis cliquez sur OK.

7. Sélectionnez Setup, Notifier Rules.

8. Dans la boîte de dialogue Notifier Manager, cliquez sur New.



9. Dans la boîte de dialogue Notifier Rule Editor, effectuez les opérations suivantes :

    a. Dans le champ Name, saisissez SPECTRUM.

    b. Dans la liste Action, sélectionnez Send Trap.

    c. Dans la liste To NMS, sélectionnez le SpectroSERVER spécifié à l'étape 4.

    d. Sous When an alarm is, sélectionnez Raised and Cleared.

    e. Sous Elements within, indiquez un type spécifique de technologie ou All Tech/Subjects.

    f. Cliquez sur OK pour enregistrer votre règle de notification.

10. Vérifiez son affichage, puis fermez la fenêtre.

Personnalisation et planification des rapports de santé pour transférer des traps

Un rapport de santé évalue l'intégrité d'un groupe d'éléments en comparant les performances actuelles aux historiques sur une journée, une semaine ou un mois. Le rapport identifie les erreurs, les taux d'utilisation inhabituels ou les variations de volume exigeant un examen.

Utilisez ce rapport pour évaluer l'intégrité de vos ressources en surveillant l'efficacité de leur exécution, en vérifiant la disponibilité des ressources vitales et en détectant d'éventuels problèmes. Le rapport analyse les tendances en fonction des données historiques et calcule des moyennes à l'aide d'un profil de service.

Vous pouvez configurer des rapports de santé afin de transférer des traps concernant des exceptions d'intégrité sur le SpectroSERVER. Pendant l'exécution d'un rapport de santé planifié, *e*Health envoie un trap SNMP au SpectroSERVER concernant le problème principal de chaque élément dans la section Exceptions du rapport de santé.

Remarque : Seuls les rapports de santé planifiés transfèrent des exceptions. Ce n'est pas le cas des rapports exécutés manuellement.

Pour transférer des exceptions à partir de rapports de santé :

1. Connectez-vous à la console *e*Health.

2. Sélectionnez Reports, Customize, Health Reports.

3. Sélectionnez le rapport à partir duquel vous souhaitez transférer les exceptions Health.

4. Dans la liste déroulante Presentation Attributes, sélectionnez General.

5. Dans le tableau Attribute, sélectionnez NMS IP et Port Trap Address.

6. Dans le champ Value, spécifiez l'adresse IP et le numéro de port SNMP du SpectroSERVER, séparés par deux-points. Exemple :

    001.02.03.004:162

7. Cliquez sur Apply pour enregistrer.



8. Dans la liste déroulante Presentation Attributes, sélectionnez Exceptions.

9. Dans le tableau Attribute, sélectionnez Send Exceptions SNMP Trap.

10. Dans le champ Value, sélectionnez Yes.

11. Cliquez sur OK.

12. Cliquez sur Save pour enregistrer le rapport personnalisé.

13. Sélectionnez Setup, Schedule Jobs.

14. Dans la liste, sélectionnez Add Health Report.

15. Dans la boîte de dialogue Add Scheduled Report, effectuez les opérations suivantes :

    a. Sélectionnez le rapport.

    b. Sélectionnez le type de technologie et le groupe du rapport afin d'en indiquer le sujet.

    c. Spécifiez la plage horaire du rapport, ainsi qu'un fuseau horaire, le cas échéant.

    d. Sélectionnez le format de sortie souhaité pour le rapport.

    e. Définissez la planification du job.

    f. Cliquez sur OK .

16. Cliquez sur OK.

Configuration d'eHealth for Voice pour envoyer des alertes à SPECTRUM

Pour que SPECTRUM OneClick affiche les problèmes de voix dans les autocommutateurs privés, les systèmes de messagerie et autres infrastructures de voix surveillées par *e*Health for Voice, configurez *e*Health for Voice Policy Manager afin d'envoyer des alertes (traps SNMP) à SPECTRUM en cas de problème. Pour configurer Policy Manager, créez une stratégie en fonction d'un plan d'action défini (réponses affectées aux stratégies) et de conditions.

Pour configurer *e*Health for Voice et envoyer des alertes à SPECTRUM :

1. Sur le système sur lequel *e*Health for Voice est installé, sélectionnez Démarrer, Programmes, *e*Health for Voice, *e*Health for Voice. La console de programmation *e*Health for Voice s'affiche.

2. Sélectionnez Tools, Service Setup pour configurer et lancer le service Policy Manager.

3. Cliquez sur Configuration, Servers pour configurer les serveurs de messagerie, SNMP, Web et SPECTRUM.



4. Définissez les actions à inclure au plan d'action :

   a. Dans le groupe Policy Manager de l'arborescence de la console, cliquez sur Templates.

   b. Cliquez sur Actions.

   c. Cliquez avec le bouton droit de la souris dans le volet droit, puis choisissez New.

   d. Renseignez les informations relatives au type d'action. Renseignez les onglets Properties et Configure.

   e. Cliquez sur Save.

   f. Cliquez sur Cancel pour fermer la fenêtre.

5. Créez un modèle de plan d'action pour définir les réponses à affecter à la stratégie :

   a. Dans le groupe Policy Manager de l'arborescence de la console, cliquez sur Templates.

   b. Cliquez sur Action Plans.

   c. Cliquez avec le bouton droit de la souris dans le volet droit et sélectionnez New.

   d. Spécifiez un nom, une description, un fuseau horaire et des actions.

   e. Cliquez sur Save.

6. Créez une stratégie en fonction de ce plan d'action :

   a. Dans le groupe Policy Manager de l'arborescence de la console, cliquez sur Policies.

   b. Pour créer une stratégie en fonction des données globales d'*e*Health for Voice, cliquez sur Global.

   c. Cliquez avec le bouton droit de la souris sur la zone vide du volet droit, puis, dans le menu contextuel, sélectionnez New.

   d. Sélectionnez Blank Policy et cliquez sur Next.

   e. Spécifiez un nom et une description.

7. Cliquez sur Add.

8. Définissez la condition :

   a. Spécifiez le nom, la plate-forme de l'élément et la table de données.

   b. Spécifiez les critères de génération.

   c. Cliquez sur Apply pour enregistrer la condition.

9. Définissez la stratégie :

   a. Sélectionnez le fuseau horaire, l'intervalle d'exploitation et le délai d'exécution.

   b. Spécifiez le nombre d'événements souhaité entre la condition et la stratégie avant le déclenchement du plan d'action.

   c. Spécifiez le niveau de gravité.

   d. Sélectionnez un plan d'action.

   e. Cliquez sur Save.



Configuration de SPECTRUM pour reconnaître le serveur *e*Health

Une fois la configuration d'*e*Health terminée, vous devez également configurer SPECTRUM pour qu'il reconnaisse le serveur *e*Health. Vous pouvez ainsi effectuer des zooms avant sur les rapports *e*Health et effacer les alarmes de la console OneClick.

Pour permettre à SPECTRUM de reconnaître le serveur *e*Health :

1. Connectez-vous à la page d'accueil SPECTRUM OneClick à l'aide de vos informations d'identification SPECTRUM et cliquez sur Administration en haut de la page.

2. Dans le menu Administration, sélectionnez *e*Health Configuration.

3. Dans la fenêtre *e*Health Configuration, entrez les informations suivantes :

    - Nom d'hôte ou adresse IP du serveur *e*Health
    - Numéro du port sur lequel *e*Health écoute les requêtes Web
    - Nom d'utilisateur de l'administrateur Web *e*Health
    - Mot de passe de l'administrateur Web *e*Health

4. Dans la section Alarm Notifier Status, sélectionnez Started pour que SPECTRUM puisse effacer les alarmes Live Health.

    Remarque : Si vous configurez *e*Health pour qu'il transfère des alarmes à SPECTRUM et ce dernier pour qu'il affiche les alarmes du premier, l'outil de notification d'alarmes vous permet d'effacer ces alarmes directement à partir de la console OneClick.

5. Cliquez sur Save.

Configuration de SPECTRUM pour afficher les alarmes *e*Health

Si vous configurez *e*Health pour qu'il transfère des alarmes Live Health ou des exceptions Health à un SpectroSERVER, vous devez également configurer SPECTRUM pour qu'il puisse recevoir ces alarmes.

Pour permettre à SPECTRUM d'afficher les alarmes d'*e*Health :

1. Connectez-vous en tant qu'administrateur de SPECTRUM.

2. En haut de la page OneClick, sélectionnez Start Console pour lancer la console OneClick.

3. Dans l'onglet Explorer du panneau de navigation OneClick, sélectionnez votre SpectroSERVER, puis Universe.

Remarque : Si vous surveillez plusieurs SpectroSERVER, sélectionnez Universe sous le paysage de Trap Director SpectroSERVER.

4. Dans le panneau Contents, sélectionnez l'onglet Topology.

5. Dans la barre d'outils de l'onglet Topology, cliquez sur l'icône Create a new model by type. La boîte de dialogue Select Model Type s'affiche.

6. Sélectionnez l'onglet All Model Types.



7. Sélectionnez EventAdmin, puis cliquez sur OK. La boîte de dialogue Create Model of Type s'affiche.

8. Spécifiez le nom et l'adresse IP du serveur *e*Health, puis cliquez sur OK. Le serveur *e*Health apparaît dans la topologie en tant que modèle EventAdmin.

Remarque : Pour plus d'informations sur la création d'un modèle dans OneClick, consultez le manuel *Modeling Your IT Infrastructure Administrator Guide*.

9. Sélectionnez le modèle EventAdmin dans la topologie OneClick.

10. Cliquez sur ce dernier avec le bouton droit de la souris, puis sélectionnez Utilities, Attribute Editor. La boîte de dialogue Attribute Editor s'affiche.

11. Dans l'arborescence Attributes, sélectionnez User Defined et cliquez sur Add. La boîte de dialogue Attribute Selector s'affiche.

12. Dans la fenêtre Select Model Type, choisissez Other, EventAdmin.

13. Dans la fenêtre Attributes for EventAdmin, sélectionnez map_traps_to_this_model_using_IP_header et cliquez sur OK. L'attribut apparaît dans la liste User Defined de la boîte de dialogue Attribute Editor.

14. Cliquez sur la flèche droite. L'attribut se déplace dans la fenêtre de droite.

15. Dans cette fenêtre, sélectionnez map_traps_to_this_model_using_IP_header, puis Yes.

16. Cliquez sur Apply. SPECTRUM applique les attributs au modèle et la boîte de dialogue Attribute Edit Results s'affiche.

17. Dans la fenêtre Attribute Edit Results, vérifiez vos changements et cliquez sur Close.

18. Dans la boîte de dialogue Attribute Editor, cliquez sur OK.

Maintenance du système

Il est préférable de sauvegarder fréquemment vos systèmes *e*Health, OneClick, SPECTRUM et *e*Health for Voice. Une sauvegarde régulière garantit une récupération rapide du système en cas d'échec du disque, de corruption de la base de données ou de tout autre événement inattendu. Sans stratégie de sauvegarde, vous risquez de passer des heures, voire des jours, à réinstaller et reconfigurer ces applications, ce qui peut engendrer la perte de données précieuses.

Pour obtenir une description complète de la gestion des sauvegardes du système et des bases de données de ces produits, reportez-vous aux manuels suivants :

- **SPECTRUM :** *Database Management*
- ***e*Health :** e*Health Database Management Guide*
- ***e*Health for Voice :** e*Health for Voice Operations Guide*



Archives des sauvegardes système

Elaborez des procédures consistant à copier les sauvegardes sur une bande ou un autre système d'un répertoire appartenant à un utilisateur fiable possédant des autorisations de lecture seule. Tous les utilisateurs ayant accès à la base de données enregistrée peuvent la restaurer sur un autre système et visualiser son contenu intégral. Pour une récupération en toute sécurité, déplacez les données archivées à l'extérieur. Investir dans une solution de stockage à distance (par exemple, celles proposées par CA BrightStor) peut s'avérer judicieux et relègue la gestion des bibliothèques de bandes en arrière-plan. Nous vous conseillons de conserver les sauvegardes archivées pendant plusieurs mois afin de bénéficier d'une vaste plage de récupération des données et des rapports. Vous pourrez ainsi récupérer vos données si une corruption s'est produite plusieurs mois auparavant sans avoir été détectée.

Recommandations de récupération de données

Il est conseillé de répéter la récupération de données sur un ordinateur test, de manière à vous familiariser avec les procédures avant d'affronter une crise.



(Page laissée vide intentionnellement)



Chapitre 6 : Collecte d'informations système à partir des agents

Les systèmes sont des composants importants du réseau. Ils contiennent généralement vos applications métier vitales, telles que les serveurs Web, les applications de bases de données, de messagerie, etc. Lorsque leurs performances se détériorent, les utilisateurs sont incapables d'exécuter leurs applications et d'effectuer les tâches nécessitant l'utilisation de ces serveurs. Le présent chapitre indique comment collecter des informations système et présente les recommandations de configuration de SPECTRUM et d'eHealth et de gestion d'Unicenter NSM, de SystemEDGE et des agents système tiers.

Déploiement et administration des agents système

SPECTRUM et *e*Health exploitent des agents de surveillance système dans le but d'obtenir des informations sur les défaillances et les performances. Le présent chapitre décrit trois types d'agents système :

- Agents CA Unicenter NSM
- Agents CA SystemEDGE
- Agents tiers

Important : Les procédures d'installation des agents Unicenter NSM et SystemEDGE sont décrites en détail dans les manuels d'installation correspondants. **Consultez ces manuels pour installer correctement les agents.** Une fois le logiciel installé, lisez le présent chapitre pour connaître les recommandations de configuration de SPECTRUM et d'*e*Health afin d'exploiter au mieux ces agents.

Recommandations

Pour faciliter la surveillance et la gestion des agents système, suivez les recommandations ci-dessous :

- Assurez-vous que l'agent système a été installé avec succès.
- Configurez une chaîne de communauté SNMP en lecture seule ou en lecture/écriture sur le système.
- Configurez l'agent système pour qu'il envoie des traps au SpectroSERVER.
- Vérifiez que vous avez spécifié l'adresse IP et la chaîne de communauté appropriées pour découvrir les agents.
- Vérifiez que vos systèmes possèdent un seul agent de gestion activé et en exécution. Parfois, les systèmes peuvent contenir plusieurs agents SNMP. Par exemple, ils peuvent comporter l'agent SNMP Microsoft et un agent CA SystemEDGE. Si plusieurs agents en exécution répondent aux exigences SNMP, SPECTRUM et *e*Health peuvent modéliser les deux agents pour le même système. Pour plus d'informations, reportez-vous à la section Agents Unicenter NSM plus loin dans ce chapitre.



Agents pris en charge

Le tableau ci-dessous met en évidence les agents Unicenter NSM pris en charge par *e*Health et SPECTRUM en fonction de la version. Les agents de performances et Active Directory servent uniquement à la génération de rapports *e*Health.

Agents des systèmes Unicenter NSM r1	Agents des systèmes Unicenter NSM 3.1
Agent système UNIX (caiUxsA2)	Agent système UNIX (caiUxOs)
Agent système Windows (caiWinA3)	Agent système Windows (caiW2kOs)
Agent Active Directory (caiAdsA2)	Agent Active Directory (caiAdsA2)
Agent de journal (caiLogA2)	Agent de journal (caiLogA2)
Agent de performances (hpxAgent)	Agent de performances (hpxAgent)

SPECTRUM et *e*Health prennent également en charge tous les agents SystemEDGE, ainsi que de nombreux agents tiers proposés par des fournisseurs tels que Microsoft, Dell, Sun, HP et IBM. De plus, ces applications prennent également en charge tous les agents compatibles avec MIB-II ou RFC 2790. Elles offrent une gestion des défaillances automatisée et prête à l'emploi, une prise en charge des traps, ainsi que la génération de tendances et de rapports sur les performances.

Remarque : Outre les performances des systèmes hôtes de base, SPECTRUM peut surveiller les processus, les systèmes de fichiers et le fichier journal des agents compatibles avec les extensions RFC 2790 de MIB-II. Si vous découvrez des agents qui ne possèdent pas d'extension RFC 2790, seule la surveillance du fichier journal et des performances des systèmes hôtes de base est possible.

Conditions préalables

Avant de commencer, effectuez les opérations suivantes :

- Vérifiez que vous possédez les autorisations d'accès au compte administrateur des consoles SPECTRUM OneClick et *e*Health.
- Pour vous familiariser avec la console SPECTRUM OneClick, reportez-vous au manuel *OneClick Administration Guide* pour plus d'informations.
- Pour vous familiariser avec les interfaces d'*e*Health, consultez les descriptions des consoles *e*Health et OneClick for *e*Health (OneClickEH) incluses dans le manuel *eHealth Administration Overview Guide*.



Ajout d'agents système dans SPECTRUM

Vous pouvez utiliser l'une des méthodes suivantes pour ajouter les agents système à SPECTRUM :

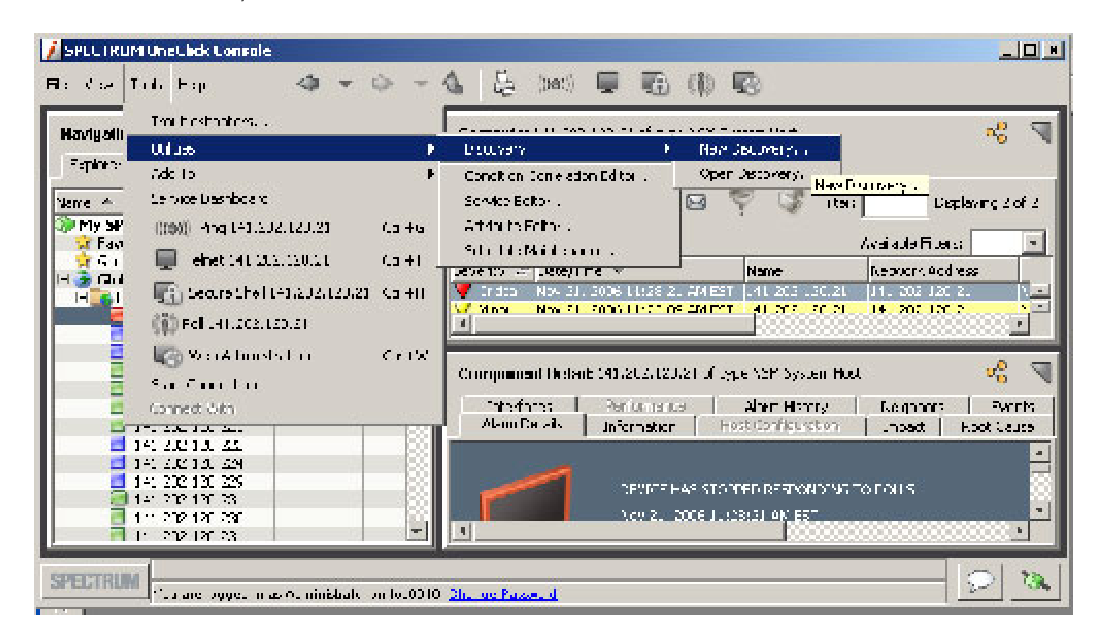
- Découvrez automatiquement les agents système à l'aide de l'application AutoDiscovery de SPECTRUM.
- Ajoutez manuellement les agents système à SPECTRUM.

DÉCOUVERTE AUTOMATIQUE D'AGENTS SYSTÈME

Les fonctions de découverte automatique de SPECTRUM vous permettent de découvrir et de modéliser automatiquement vos ressources système.

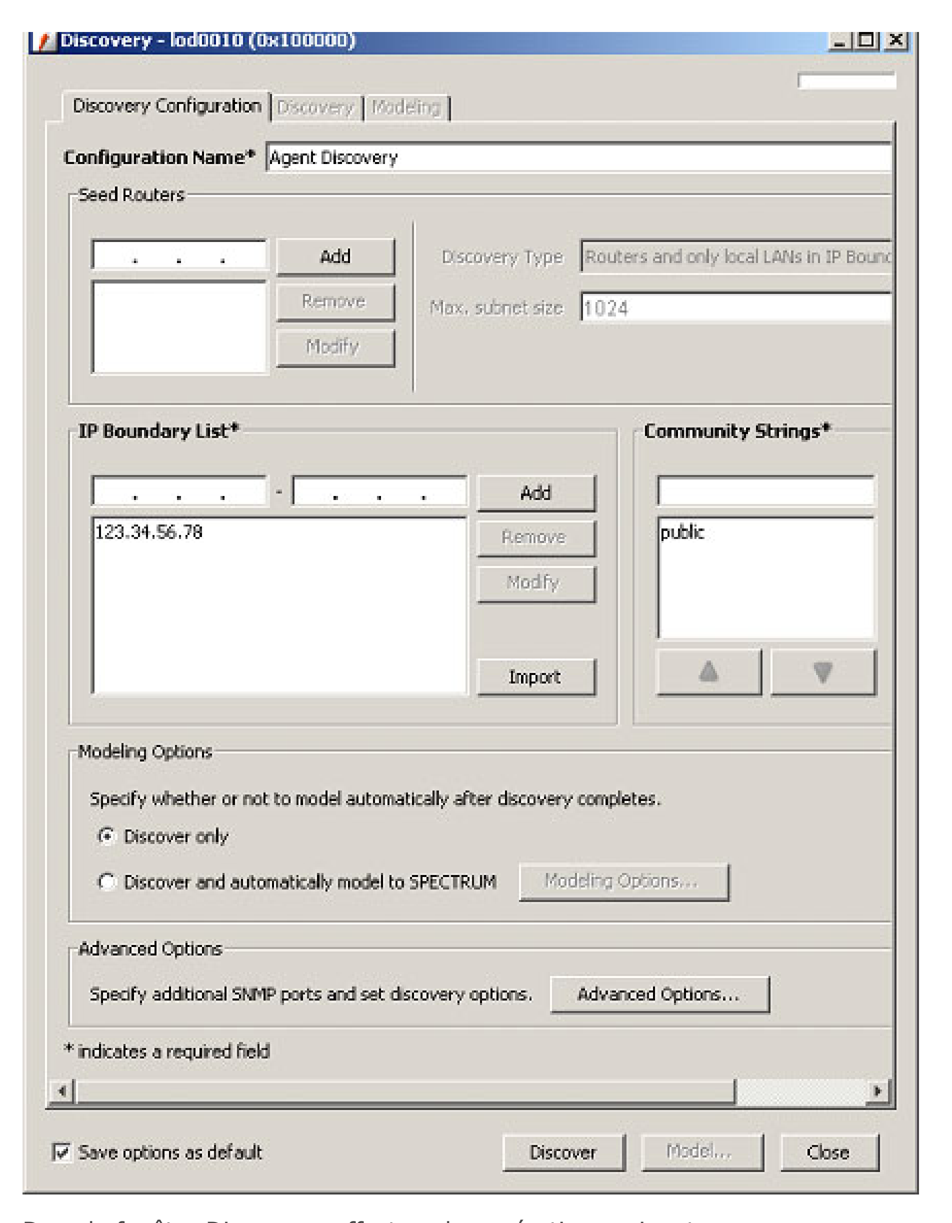
Pour découvrir automatiquement vos systèmes :

1. Dans la console SPECTRUM OneClick, sélectionnez Tools, Utilities, Discovery, New Discovery.



La boîte de dialogue Discover s'affiche.



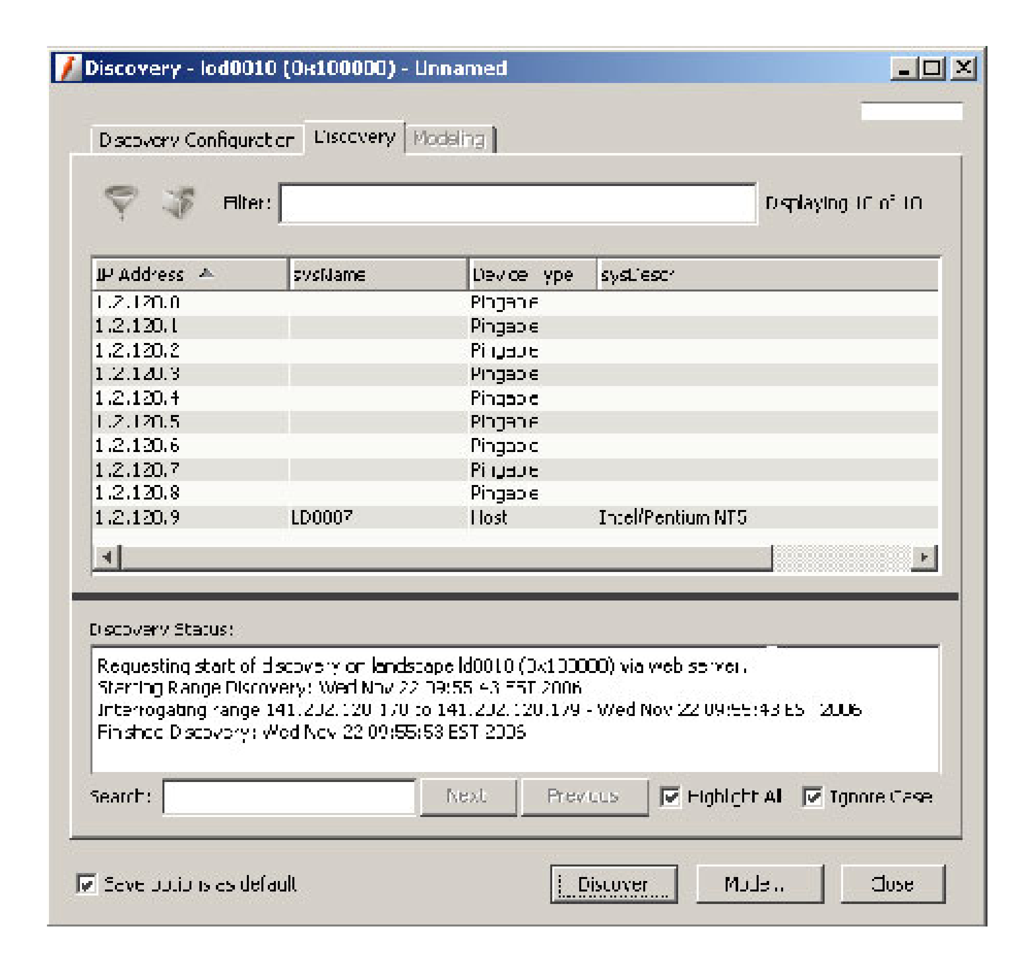


2. Dans la fenêtre Discovery, effectuez les opérations suivantes :

   - Spécifiez un nom de configuration.
   - Spécifiez une liste ou une plage d'adresses IP, ou sélectionnez Import pour importer un fichier de liste d'adresses IP.
   - Spécifiez une chaîne de communauté valide. Si vous en spécifiez plusieurs, OneClick utilise la première entrée de la liste.
   - Dans Modeling Options, sélectionnez Discover Only.
   - Cliquez sur Advanced Options et spécifiez le port 6665 pour découvrir les agents Unicenter NSM.

3. Cliquez sur Discover. La boîte de dialogue Discovery apparaît.

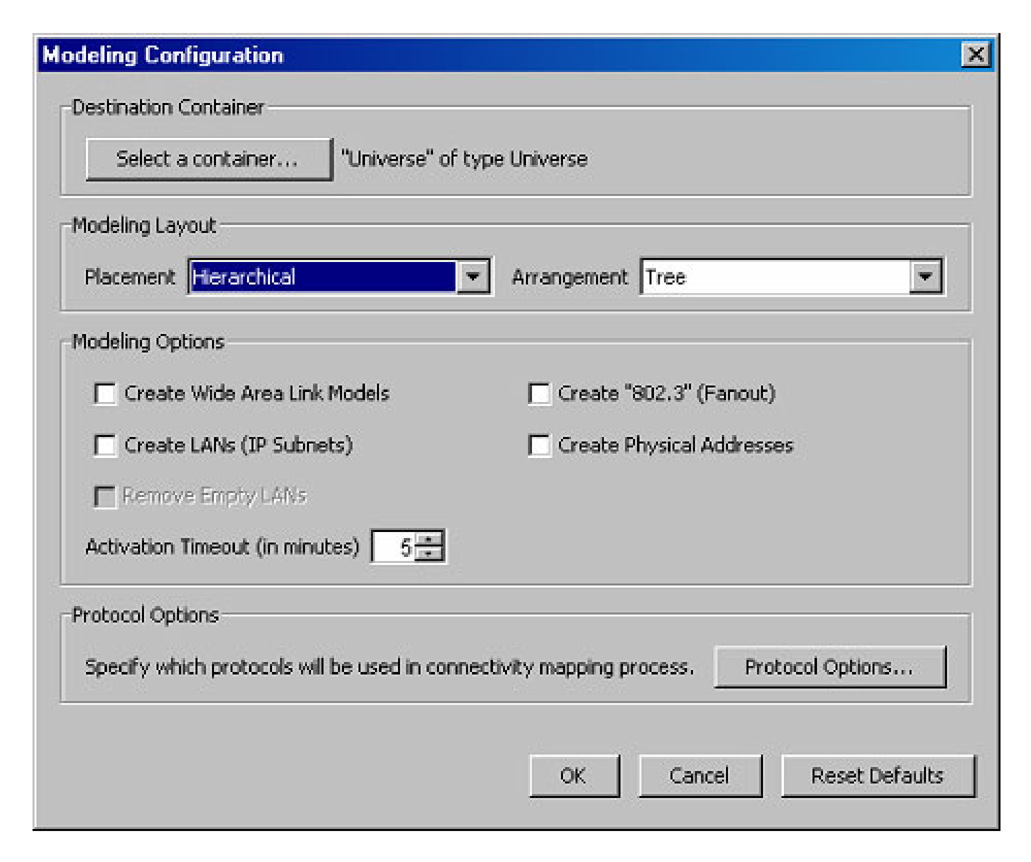




4. (Facultatif) Une fois les résultats affichés, excluez des entrées en cliquant dessus avec le bouton droit et en sélectionnant Exclude. Les périphériques correspondants ne sont pas modélisés dans la base de données SPECTRUM.

5. Cliquez sur Model pour ajouter les systèmes à SPECTRUM.



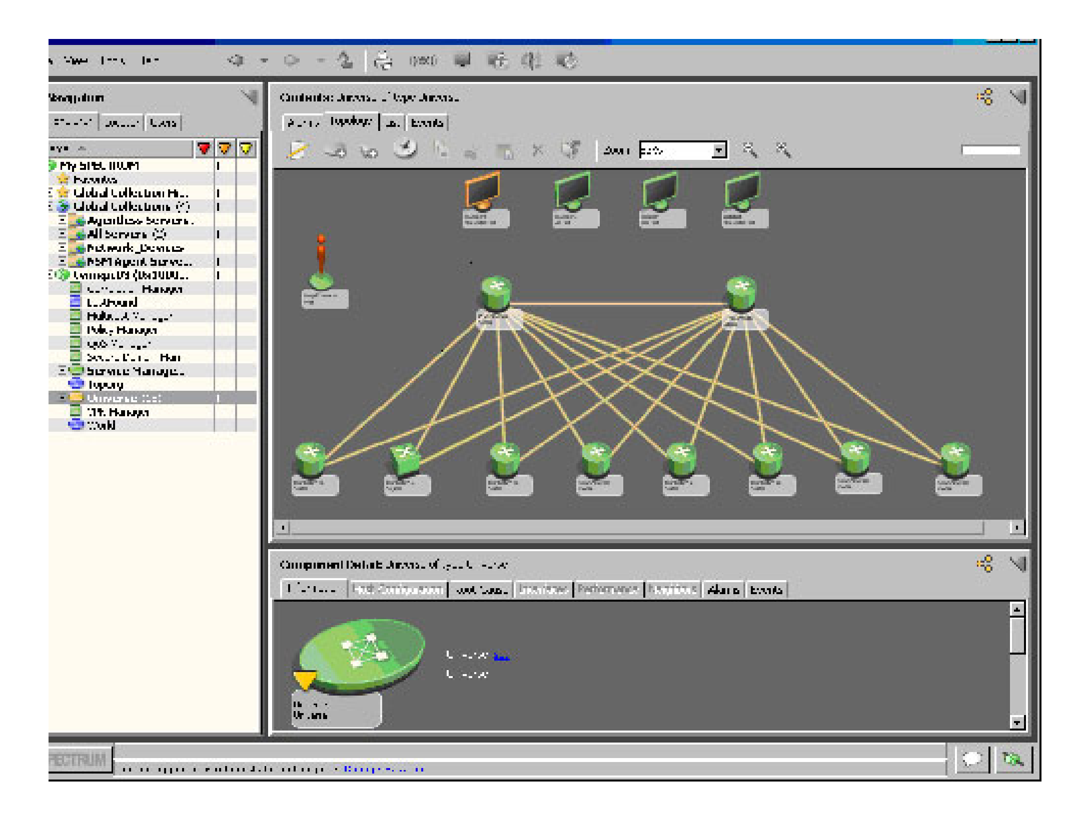


6. Dans Modeling Options, désactivez les options Create Wide Area Link Models et Create LANs. Lorsque ces options sont désactivées, SPECTRUM ne crée pas automatiquement de conteneurs de sous-réseau. Pour plus d'informations sur les options de découverte et de modélisation, reportez-vous au *Modeling Your IT Infrastructure Administrator Guide*.

7. Cliquez sur OK.

8. Après la modélisation des systèmes, cliquez sur Close dans la boîte de dialogue Discovery.





9. (Facultatif) Dans le coin gauche du menu Outils, cliquez sur l'icône représentant une feuille avec un crayon.
10. Modifiez la topologie en déplaçant les icônes et ajoutez les images d'arrière-plan de votre choix.

AJOUT MANUEL D'UN PÉRIPHÉRIQUE VIA LA BOÎTE DE DIALOGUE CREATE MODEL BY IP ADDRESS

Au lieu de lancer la découverte automatique de vos systèmes, vous pouvez les modéliser manuellement. Cette procédure fonctionne pour les systèmes qui ne prennent pas en charge les découvertes.

Pour modéliser manuellement vos ressources système :

1. Dans l'onglet Explorer du volet de navigation OneClick, accédez à la vue de topologie Universe à laquelle vous voulez ajouter le nouveau périphérique. La vue sélectionnée apparaît dans l'onglet Topology du panneau Contents. **Astuce :** Si vous souhaitez placer le nouveau périphérique dans un conteneur de groupe réseau, double-cliquez sur l'icône du conteneur pour afficher la vue de topologie de ce conteneur.
2. Dans la barre d'outils de l'onglet Topology, cliquez sur le bouton Create model by IP address. La boîte de dialogue Create model by IP address apparaît.



Remarque : Pour supprimer un élément modélisé d'une vue, sélectionnez l'élément et cliquez sur *Delete (***X***).*



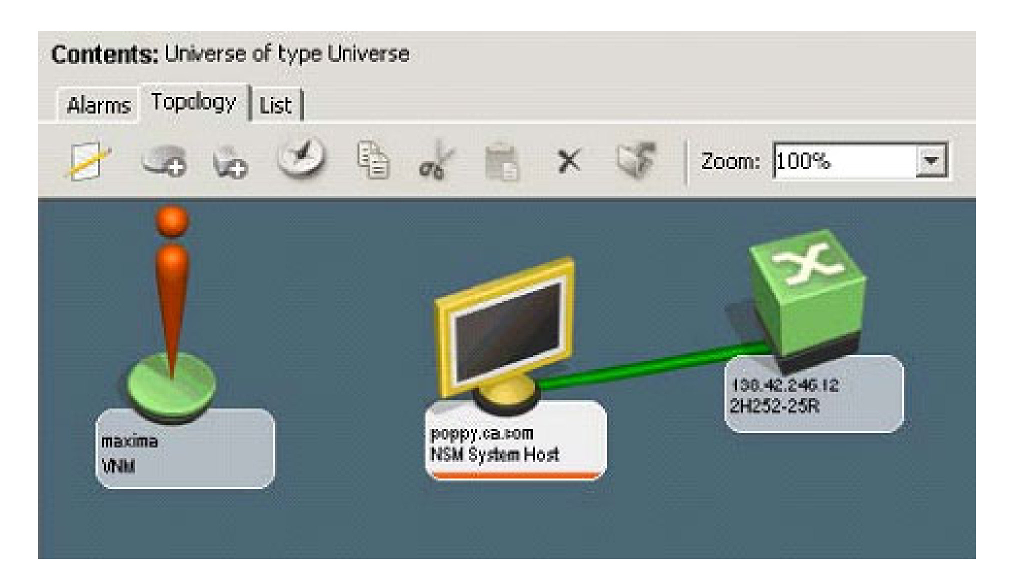
3. Spécifiez l'adresse réseau du périphérique et tout autre champ facultatif décrit dans le tableau suivant.

Create Model by IP Address

Champ	Description
Network Adress (obligatoire)	Indique l'adresse réseau (adresse IP) du périphérique à modéliser.
Community Name (obligatoire)	Indique la chaîne de communauté SNMP du périphérique à gérer.
DCM Timeout (facultatif)	Indique la durée pendant laquelle Assurance Server doit attendre la réponse du périphérique. La valeur par défaut est 3 000 ms.
DCM Retry Count (facultatif)	Indique la fréquence à laquelle Assurance Server essaie de communiquer avec le périphérique après expiration de la valeur de temporisation DCM. La valeur par défaut est 2.
Agent port (facultatif)	Indique le port sur lequel l'agent écoute les requêtes SNMP. La valeur par défaut est 161. Les agents Unicenter NSM utilisent le port 6665.
SNMP v2C Enabled (facultatif)	Indique si le périphérique en cours de modélisation prend en charge les protocoles SNMPv2c. Sélectionnez cette option si vous modélisez un périphérique configuré pour SNMP v2C.
SNMP v3 Enabled (facultatif)	Indique si le périphérique en cours de modélisation prend en charge les protocoles SNMPv3c. Sélectionnez cette option si vous modélisez un périphérique configuré pour SNMP v3.
Discover connections (facultatif)	Permet à SPECTRUM OneClick de découvrir les connexions établies (canaux) entre le périphérique (que vous ajoutez) et ses voisins.

4. Dans la boîte de dialogue Create Model by IP Address, cliquez sur OK pour créer l'icône du périphérique spécifié (ou cliquez sur Cancel pour annuler l'opération de modélisation par IP). Lorsque vous cliquez sur OK, SPECTRUM OneClick place la nouvelle icône du périphérique dans la vue de topologie Universe sélectionnée.





Astuces : Pour déplacer la nouvelle icône ou améliorer son apparence, cliquez sur le bouton du mode Edit dans la barre d'outils de l'onglet Topology. Vous pouvez modifier et réorganiser les périphériques modèles à l'aide des techniques suivantes.

- Pour copier ou coller l'icône du périphérique modélisé dans une vue de topologie autre que celle d'Universe, utilisez les fonctions de copier/coller dans la barre d'outils de l'onglet Topology.
- Pour modifier les paramètres de configuration d'un périphérique modélisé (ex : nom de communauté, intervalle entre les interrogations, intervalle entre les journalisations, chaîne de sécurité, etc.), sélectionnez le périphérique et modifiez les paramètres appropriés dans le panneau Component Detail.

Agents Unicenter NSM

Vous pouvez découvrir et modéliser automatiquement les agents Unicenter NSM en utilisant la fonction de découverte SPECTRUM. Vous pouvez également les modéliser manuellement. Par défaut, les agents Unicenter NSM utilisent le port UDP 6665 pour les communications SNMP plutôt que le port SNMP standard 161. SPECTRUM peut donc découvrir et modéliser d'autres agents en cours d'exécution sur le périphérique hôte. Par exemple, si une station de travail Windows exécute un agent Unicenter NSM lié au port 6665, ainsi que l'agent SNMP Microsoft lié au port 161, SPECTRUM crée deux modèles de périphérique nommés Unicenter NSM System Host et Windows Host, comme indiqué dans la figure suivante.





Ce scénario peut entraîner une diminution des performances pour les raisons suivantes.

- Il crée des modèles redondants inutiles dans SPECTRUM.
- Il entraîne une interrogation et un trafic SNMP redondants pouvant réduire les performances du réseau et de SPECTRUM.
- Il réduit les performances de l'ordinateur hôte de l'agent car plusieurs agents de gestion fournissent des données de performances.

Pour éviter ce scénario, procédez comme suit :

1. Avant la découverte et la modélisation, arrêtez et/ou supprimez tous les agents de gestion sauf celui à utiliser pour gérer le système. Vous évitez ainsi de créer et de gérer plusieurs modèles pour le même hôte dans SPECTRUM. Pensez à utiliser le port SNMP adéquat pour la découverte.

2. Si vous devez exécuter plusieurs agents sur un système hôte donné, vous pouvez modéliser manuellement uniquement l'agent à gérer avec SPECTRUM.

Ajout d'agents système dans *e*Health

Après avoir découvert et modélisé les systèmes avec SPECTRUM, importez une collection globale SPECTRUM pour ajouter ces ressources système à *e*Health à des fins de génération de rapports et de surveillance Live Health. Vous pouvez également ajouter les systèmes à l'aide d'*e*Health Discovery, mais il est préférable d'importer les systèmes depuis SPECTRUM, comme décrit au chapitre 5. Après quelques cycles d'interrogation *e*Health, vous pouvez exécuter des rapports At-a-Glance et Trend depuis l'interface OneClick.

Rapports de performance des agents système

*e*Health normalise les données de performances communes sur l'ensemble des agents système gérés (Unicenter NSM, SystemEDGE et tiers). La présentation des données de performances dans un format commun et compréhensible réduit le temps d'apprentissage de tous les utilisateurs ayant accès aux rapports de tendance historiques et en temps réel.

Rapports At-a-Glance

Un rapport *e*Health At-a-Glance pour les éléments système fournit des statistiques récapitulatives sur la capacité du système spécifié, notamment l'unité centrale, l'interface et l'utilisation de la partition, les erreurs de disque et l'E/S ainsi que la disponibilité du système. Ces rapports vous permettent d'isoler rapidement les UC occupées ou les disques pleins et de comparer les groupes de systèmes. Un exemple de rapport At-a-Glance est fourni ci-dessous.



At-a-Glance Report

Unix Server

SysEdge UNIX System Element rainbow-SH

CPU Utilization

100% 80% 60% 40% 20% 0%

CPU Load Average (processes)

1.5 1 0.5 0

Server Availability

100% 80% 60% 40% 20% 0%

Physical Memory (bytes)

300M 250M 200M 150M 100M 50M 0

Total Used

Virtual Memory (bytes)

2G 1.5G 1G 500M 0

Total Used

Page Faults (page faults/sec)

180 140 100 60 20

Page Scan Rate (pages/sec)

45 35 25 15 5

24-Apr-01 3:31 PM 7:31 PM 11:31 PM 05-Apr-01 3:31 AM 7:31 AM 11:31 AM 3:31 PM

Time

Disk I/O (reads&writes/sec)

3.5 1

Reads Writes

Disk I/O Busy Utilization

4% 2% 0%

Disk I/O Queue Length (reads&writes)

1 0.4

Disk Errors (errors/sec)

1 0.4

User Partition Space Used (bytes)

30G 15G 0

Capacity Used

System Partition Space Used (bytes)

25G 10G

Capacity Used

Total Network I/O (frames/sec)

350 100

600 200

In Out

Total Network Errors (errors/sec)

1 0.4

1 0.4

In Out

Server Latency (msec)

1 0.4

24-Apr-01 3:31 PM 7:31 PM 11:31 PM 05-Apr-01 3:31 AM 7:31 AM 11:31 AM 3:31 PM

Time



EXÉCUTION DE RAPPORTS AT-A-GLANCE

Vous pouvez exécuter des rapports At-a-Glance en suivant l'une de ces méthodes :

- Dans SPECTRUM OneClick, cliquez avec le bouton droit de la souris sur un périphérique, puis cliquez sur At-a-Glance Reports. Le rapport At-a-Glance intégré s'exécute en arrière-plan et apparaît automatiquement dans un navigateur Web sur votre système.
- Avec un navigateur Web, connectez-vous à l'interface Web *e*Health à l'adresse suivante : http://*hostname*:*port*, où *hostname* représente le nom ou l'adresse IP de votre système *e*Health et *port* correspond au port HTTP utilisé par le serveur Web. Si le serveur Web utilise le port 80 par défaut, vous pouvez omettre le numéro de port. Pour vous connecter à l'interface Web *e*Health, vous devez posséder un compte utilisateur Web *e*Health. Accédez à l'onglet Run Reports et exécutez un rapport At-a-Glance sur demande.

Rapports MyHealth pour les systèmes

La page MyHealth report de l'interface Web d'*e*Health contient une série de graphiques qui vous sont spécialement destinés. MyHealth fournit aux utilisateurs Web d'*e*Health un ou plusieurs rapports personnalisés sur les éléments et les groupes qu'ils considèrent comme vitaux. Une page de rapport MyHealth contient un ou plusieurs panneaux, chacun présentant un graphique séparé.

Rapports *e*Health pour les systèmes

Un rapport *e*Health contient des informations sur les performances d'un groupe d'éléments pendant une période spécifique et attire votre attention en cas de nécessité. Le rapport identifie également les situations à rechercher en cas d'erreurs, de taux d'utilisation inhabituels ou de volume excessif.

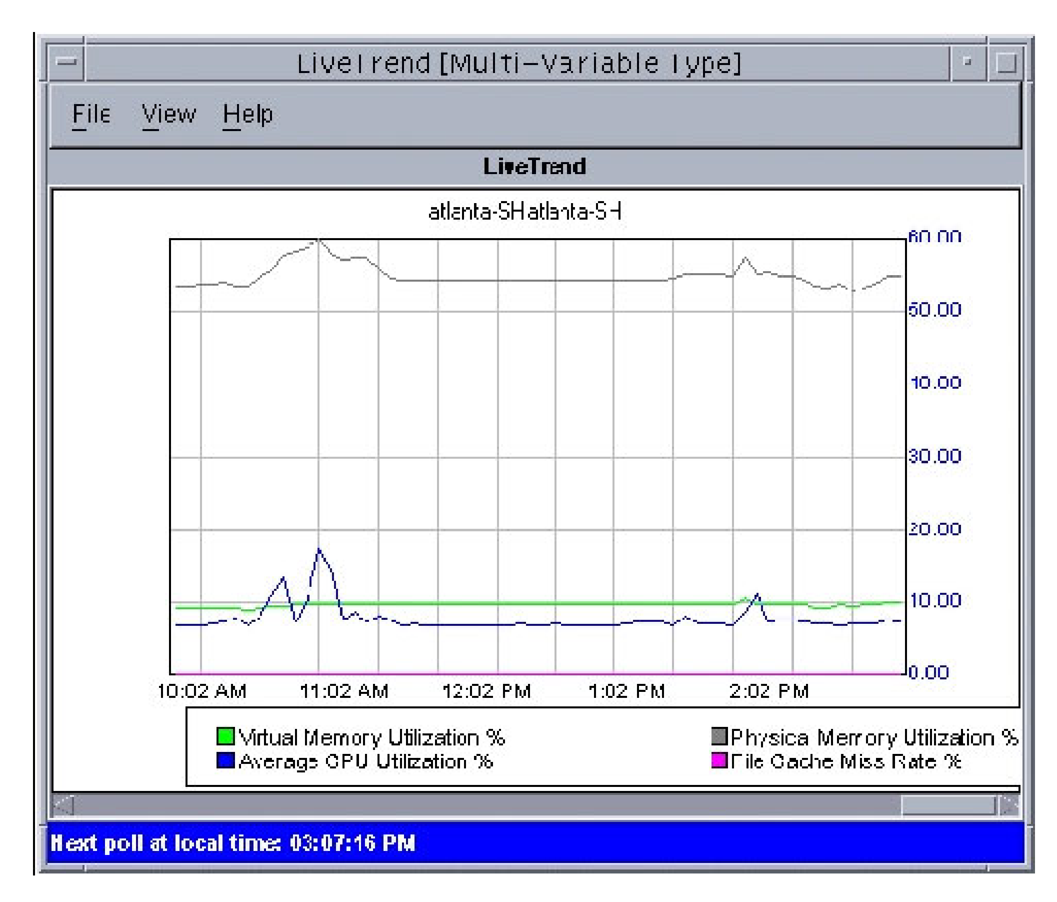
Vous pouvez utiliser un rapport Health pour effectuer les opérations suivantes :

- Identifier les comportements normaux et exceptionnels du système
- Comparer les performances d'un groupe d'éléments pendant une période spécifique à celles d'une période de référence
- Détecter les changements de comportement qui traduisent des problèmes imminents ou existants
- Identifier les tendances en termes de volume
- Identifier les systèmes qui nécessitent un examen plus approfondi

Utilisation de Live Trend

Live Trend permet de créer des graphiques surveillant les éléments de statistiques que vous interrogez à l'aide d'*e*Health. Vous pouvez créer un ou plusieurs graphiques dans différents styles pour représenter des tendances d'élément (un seul élément avec plusieurs variables) ou des tendances de variable (une seule variable pour plusieurs éléments). Le graphique Live Trend ci-dessous présente quatre variables sur un système appelé atlanta.





DÉMARRAGE DE LIVE TREND

Pour utiliser Live Trend, vous devez vous connecter à l'interface Web d'*e*Health et télécharger l'application cliente Live Health sur votre station de travail ou PC local. Installez le client Live Health en suivant les instructions fournies sur la page de téléchargement. Vous pouvez ensuite lancer l'application Live Trend pour exécuter les graphiques de performances en temps réel de vos systèmes et ressources.

Pour lancer l'application Live Trend :

1. Vérifiez que le logiciel client Live Health a été téléchargé et installé à partir de l'interface Web *e*Health.
2. Pour ouvrir l'application Live Trend, procédez comme suit :
   - Si vous utilisez un système Windows, sélectionnez Démarrer, Programmes, *e*Health, Live Trend. Le nom du groupe de programmes varie en fonction du nom utilisé à l'installation du client Live Health.
   - Sur un système UNIX, accédez au répertoire d'installation du client Live Health et exécutez la commande nhLiveTrend.
3. Dans le champ *e*Health System de la fenêtre d'application Live Trend, spécifiez le nom du système auquel vous souhaitez vous connecter, ainsi que votre nom d'utilisateur et mot de passe. La fenêtre Live Trend Chart Definition Manager apparaît.

Vous pouvez créer vos propres graphiques grâce au Live Trend Chart Definition Editor et spécifier les éléments et les variables dont vous souhaitez afficher les données. Pour plus d'informations, reportez-vous à l'aide en ligne Live Trend accessible depuis l'interface Web d'*e*Health.



Exécution de rapports de tendance pour les systèmes

Vous pouvez utiliser les rapports de tendance pour déterminer la valeur d'une ou de plusieurs variables système sur une période spécifiée. Vous pouvez ainsi suivre les valeurs des variables et déterminer le moment où elles ont radicalement changé ou celui où un événement particulier, comme un redémarrage ou une interrogation manquée, est survenu.

Les variables de tendance diffèrent pour chaque type d'élément. Vous pouvez exécuter des rapports pour les types et les composants de système suivants :

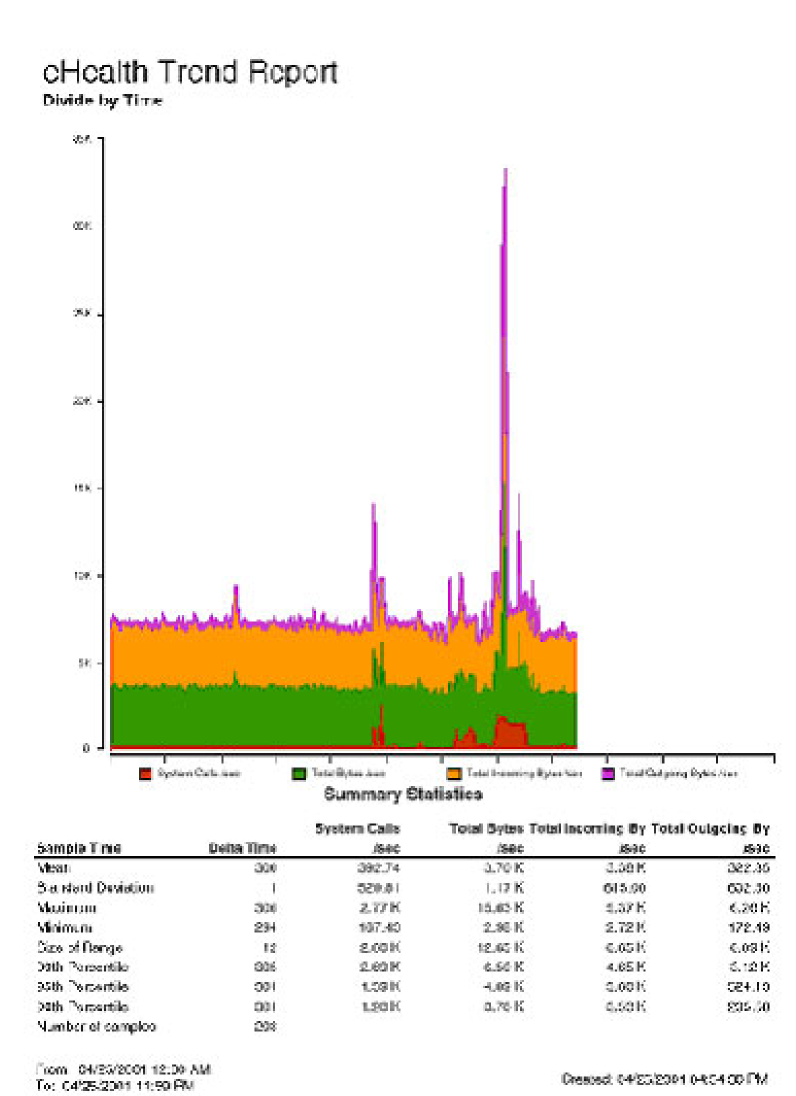
- UC
- Disque
- Réseau local
- Processus et ensemble de processus
- Utilisateur ou partition du système
- Réseau étendu

Chacun de ces types inclut des variables spécifiques sur lesquelles vous pouvez exécuter des rapports. Par exemple, les éléments de disque du serveur comportent des variables pour les lectures et écritures de disque, la capacité de stockage et l'utilisation du stockage. Vous pouvez sélectionner simultanément jusqu'à dix variables sur lesquelles vous pouvez exécuter un rapport de tendance. Pour consulter la liste exhaustive des variables Trend du système, reportez-vous à l'aide en ligne d'*e*Health.

L'exemple de rapport de tendance suivant présente plusieurs variables système communes :

- Total Bytes (Total des octets)
- Total Incoming Bytes (Total des octets entrants)
- Total Outgoing Bytes (Total des octets sortants)
- System Calls (Appels système)





Sample Time	Delta Time	System Calls /sec	Total Bytes /sec	Total Incoming By /sec	Total Outgoing By /sec
Mean	300	392.74	3.70 K	3.38 K	322.35
Standard Deviation	1	529.81	1.17 K	615.00	602.30
Maximum	306	2.77 K	15.63 K	5.37 K	6.20 K
Minimum	294	107.40	2.98 K	2.72 K	172.49
Size of Range	12	2.66 K	12.65 K	6.05 K	6.03 K
99th Percentile	306	2.60 K	6.56 K	4.65 K	6.12 K
95th Percentile	301	1.59 K	4.09 K	3.60 K	524.10
90th Percentile	301	1.26 K	3.76 K	3.53 K	295.50
Number of samples	298				

From 04/25/2001 12:00 AM
To: 04/25/2001 11:59 PM

Created: 04/25/2001 04:04:00 PM

EXÉCUTION D'UN RAPPORT DE TENDANCE

Vous pouvez exécuter les rapports de tendance depuis l'interface Web d'eHealth.

Pour créer un rapport de tendance similaire à l'exemple ci-dessus :

1. Connectez-vous à l'interface Web d'eHealth à partir d'un navigateur Web.
2. Cliquez sur l'onglet Run Reports.
3. Dans le cadre Available Reports, faites défiler le curseur jusqu'à la section Trend reports.
4. Cliquez sur Standard.
5. Sélectionnez le type d'élément système.
6. Dans la liste Elements, sélectionnez l'élément système cible.



7. Dans la liste Variables, sélectionnez des variables ; l'exemple montre les quatre variables Total des octets, Total des octets entrants, Total des octets sortants et Appels système.
8. Sélectionnez le type de graphique (ex : ligne empilée).
9. Faites défiler le curseur du cadre à droite et cliquez sur More Options.
10. Dans l'onglet General, sélectionnez Show Summary Statistics pour afficher les données tabulaires sous le graphique.
11. Cliquez sur Generate Report. *e*Health traite les données du rapport et affiche le rapport de tendance.

Rapports N premiers

Un rapport Top N (N premiers) répertorie tous les éléments d'un groupe supérieurs ou inférieurs aux objectifs de critères de rapport spécifiés. Vous pouvez également spécifier l'objectif de chaque variable. *e*Health calcule la différence entre la valeur réelle de cette variable et l'objectif défini.

Rapports What-If Capacity Trend pour les systèmes

Le rapport *e*Health What-If Capacity Trend vous permet d'exécuter une planification de la capacité en ajustant les facteurs de capacité et de demande jusqu'à trouver la solution de simulation appropriée. Ce rapport vous permet d'illustrer des scénarios futurs possibles et donc, de vous préparer aux problèmes avant que ceux-ci ne surviennent.



Chapitre 7 : Gestion des niveaux de service

La solution CA a été développée autour d'un concept appelé Business Service Intelligence (BSI), une méthodologie qui permet de comprendre les relations et l'impact de l'infrastructure informatique sur les services métier. BSI assure la fonction Technology Relationship Mapping, ainsi que l'analyse d'impact et de la cause première, ce qui permet à nos clients d'améliorer leurs services informatiques. Ils peuvent ainsi passer d'une approche tactique réactive à une approche stratégique proactive et améliorent la qualité de leur service informatique d'un point de vue interne comme externe.

BSI fournit une analyse adaptative qui communique dans les deux sens avec des milliers de périphériques multifournisseurs et multitechnologiques pour identifier, vérifier et résoudre les problèmes complexes à l'aide de moteurs de corrélation basés sur des modèles, des règles et des stratégies. L'automatisation simplifie la définition des services métier et la maintenance continue, alors que l'utilisation des ressources, la disponibilité, la planification de la capacité, la gestion des modifications, les performances et l'analyse de tendance valident le respect des contrats de niveau de service. BSI fournit une approche ascendante de Business Service Management (BSM) qui s'avère pratique, réalisable et rapidement rentable.

BSM offre la valeur ajoutée la plus évidente lorsque les données de gestion des défaillances de base sont insuffisantes et qu'elles nécessitent une corrélation supplémentaire pour déterminer l'impact possible d'une erreur et pour identifier les services métier touchés. Le module SPECTRUM Service Management permet d'organiser, d'analyser et de contrôler tous les aspects de ce domaine. Il vient en complément de OneClick en fournissant un tableau de bord ciblé sur l'intégrité du service. Il présente en outre une topologie bien plus simple que celle de OneClick.

En général, l'approche de la gestion de services peut être décrite comme « descendante » lorsqu'il s'agit d'identifier les relations et les dépendances des périphériques, des systèmes, des applications ou des mesures de performances. Dans SPECTRUM, elles sont appelées ressources (modèles ou données) et relations. Ces ressources et relations sont organisées en modèles de service ou de sous-service. Vous devez définir un service du bas vers le haut pour permettre la future réutilisation des services ou sous-services communs. Vous pouvez configurer des contrats de niveau de service pour mesurer les violations de manière dynamique et envoyer des alertes.

Ce chapitre décrit une approche de conception et d'implémentation d'un système de gestion de services dans l'application SPECTRUM. Contrairement à la plupart des fonctions de SPECTRUM, la préparation de la gestion de services peut impliquer une planification considérable pour déterminer l'ensemble des informations requises et des répercussions.

La méthodologie SPECTRUM est conçue pour évoluer au fil du temps. La quantité d'informations disponibles augmentant à mesure que l'implémentation progresse, il est généralement nécessaire d'obtenir une représentation plus granulaire ainsi qu'une mesure de la modélisation et de la gestion des services.

Références supplémentaires :
Service Manager User Guide
Report Manager User Guide
SERVICE Performance Manager User Guide



Procédures de demande de renseignements

Cette section décrit une méthode de conception et d'implémentation du processus de demande de renseignements pour la gestion des services.

Questions générales

Pour organiser et implémenter la gestion des services et des niveaux de service, documentez et collectez les réponses aux questions suivantes :

- Quels services métier voulez-vous surveiller ?
- Quelles ressources particulières prennent en charge ces services ?
    - Des processus ?
    - Des applications logicielles ?
    - Des périphériques informatiques ?
- Comment les conditions et les défaillances qui compromettent les services peuvent-elles être détectées ?
- Quels attributs de ressource doivent être surveillés pour déterminer l'intégrité d'un service ?
- Qui doit être averti en cas d'erreur sur un service donné ?
- Que sont les contrats de niveau de service et comment doivent-ils être quantifiés (mesures) ?
- Quelle est le niveau de gravité d'un service donné par rapport aux autres services ou sous-services ?

Questions techniques

Pour organiser et implémenter la gestion des services et des niveaux de service, documentez et collectez les réponses aux questions suivantes :

- Quelles technologies de réseau local et étendu prennent en charge le service ?
- Les CoS de la qualité de service sont-elles actuellement configurées ?
- Les VPN basés sur MPLS et actuellement utilisés sont-ils surveillés ?
- Les périphériques réseau et les serveurs vitaux sont-ils gérables et gérés ?
- Les éléments sont-ils correctement découverts et associés aux couches 2 ou 3 ?
- Les seuils sont-ils configurés sur vos interfaces vitales ?
    - Quel est le taux d'erreur ?
    - Quel est le taux de suppression ?
    - Quel est le niveau de charge, etc. ?
- Un système de surveillance de l'environnement doit-il être surveillé (température ou humidité) ?
- Un système d'alimentation ou de batterie de secours doit-il être surveillé ?
- Les fichiers journaux ou journaux d'événements Windows vitaux sont-ils surveillés ?
- Les processus ou services Windows vitaux sont-ils surveillés ?



- Les ports de l'application sont-ils testés ?
    - File Transfer Protocol (FTP) ?
    - Hypertext Transfer Protocol (HTTP) ?
    - Système de nom de domaine (DNS) ?
- Pour des besoins plus spécifiques, des alarmes/seuils personnalisés sont-ils configurés ?
- N'importe quel attribut de modèle peut-il servir à déterminer l'intégrité d'un service ?
- Des alarmes uniques ont-elles été créées à l'aide de la corrélation des événements ou des conditions ?
- Des intégrations existantes ou personnalisées sont-elles activées avec des données d'alarme utilisables ?
- Qui est responsable du bon fonctionnement de chacune des ressources informatiques répertoriées ?
- Chacun a-t-il accès aux outils adéquats et ses coordonnées (e-mail, téléphone, etc.) sont-elles disponibles en vue d'une distribution ?
- Existe-t-il un dépanneur attitré pour chaque ressource ou des dépanneurs sont-ils ajoutés pour permettre une notification correcte ?
- Quels utilisateurs profitent des ressources informatiques répertoriées ?
- Degré des relations entre les utilisateurs :
    - Bas
    - Moyen bas
    - Moyen
    - Moyen élevé
    - Elevé
- Existent-ils des groupes logiques d'utilisateurs à des fins de tri ?
    - Service
    - Fonction
    - Rôle, etc.
- Le niveau de gravité du périphérique est-il défini et/ou mesuré pour tous les périphériques et serveurs du réseau ?



Procédures d'analyse et d'association

Cette section décrit une approche d'analyse et d'association des résultats du processus de demande de renseignements lors de la gestion de services.

Mode d'organisation des informations sur les ressources

Suivez ces recommandations afin d'organiser les informations collectées pour vos services.

- Triez les informations par type, par exemple :
  - Noms d'application
  - Noms de serveur
  - Noms et/ou types de périphériques
  - Mesures et sources de données
- Identifiez les regroupements logiques de ces ressources communes afin d'éviter tout doublon.

Illustration des relations entre les ressources

Créez un graphique qui présente les relations entre les ressources. Ce graphique vous permet d'associer les impacts et les dépendances entre les ressources.

Décomposition des informations et association avec des modèles de service

Les informations collectées et préparées peuvent servir à créer des modèles de service que vous devez surveiller avec SPECTRUM.

- Envisagez une approche ascendante pour créer tout d'abord les modèles de ressources les plus communs.
- Créez un modèle de service en établissant une relation avec les modèles de sous-service appropriés.
- Ajoutez des ressources spécifiques aux services non disponibles via les sous-services.



Exemple d'association d'un service métier avec des modèles de service

Le client ABC a identifié un processus métier vital. Lorsque des clients passent commande par téléphone, les opérateurs saisissent les commandes dans un système Web de traitement des commandes. Ces commandes sont stockées et traitées depuis une base de données Oracle. De nombreux problèmes pouvant survenir au cours de ce processus, le client ABC souhaite créer un service indiquant le moment où le traitement de la commande est compromis. Lors du processus de demande de renseignements, certains éléments vitaux ont été identifiés puis regroupés dans la hiérarchie suivante :

- Serveur Web (WEBORDER1)
    - Matériel Dell, avec un agent SNMP en cours d'exécution (RFC 2790 ou équivalent)
    - Serveur Web Microsoft Internet Information Services (IIS)
    - Fichier journal avec entrées de flux de données vitales
    - UC et mémoire à surveiller
    - Batterie de secours avec alimentation sans coupure APC
    - Réponse appropriée requise du serveur Web
- Serveur de base de données Oracle (WEBDB1)
    - Matériel Dell, avec un agent SNMP en cours d'exécution (RFC 2790 ou équivalent)
    - Base de données Oracle avec agent intelligent Oracle
    - UC et mémoire à surveiller
    - Batterie de secours avec alimentation sans coupure APC
- Commutateurs Cisco 6509 Catalyst
    - DATASW1 responsable des connexions au serveur
    - DATASW2 responsable des connexions à la station de travail de l'opérateur
- 25 stations de travail d'opérateur
    - Surveillance du service DNS requise
    - Fonctionnement du service DHCP (Dynamic Host Configuration Protocol) requis

En posant des questions comme celles présentées ci-dessous, vous pouvez determiner le niveau de gravité des éléments par rapport à diverses erreurs possibles :

- Quels sont les échecs les plus graves qui pourraient survenir ?
- Est-il possible de mesurer l'ensemble des éléments choisis ?
- Quel serait le niveau de gravité d'un élément par rapport aux autres ?
- Les éléments de la liste peuvent-ils ou doivent-ils être réutilisés comme service générique pour d'autres processus métier informatiques ?
- Quels sont les processus qui serviront à gérer les problèmes ?
- Quelle situation serait la plus grave ? Perdre 25 % des stations de travail ou perdre le commutateur utilisé pour connecter les serveurs ?



Commencez par regrouper les ressources et les interruptions les plus vitales. L'échec le plus grave serait probablement la perte des serveurs ou des commutateurs. Commencez donc par regrouper les éléments comme suit :

- SERVICE : traitement Web des commandes
    - Composants : WEBORDER1, WEBDB1, DATASW1, DATASW2
        - Toute mise à l'arrêt d'un composant se répercute sur le service.
        - Les ports des commutateurs sont connectés au serveur.
        - Toute mise à l'arrêt d'un port se répercute sur le service.
    - Composants : stations de travail d'opérateur
        - Si 75 % des stations de travail sont à l'arrêt, le service l'est aussi.
        - Si 50 % des stations de travail sont à l'arrêt, le service est détérioré.
        - Si 25 % des stations de travail sont à l'arrêt, le service est légèrement détérioré.
    - Performances : temps de réponse Web, port TCP pour Oracle
        - Si les deux rencontrent une erreur critique, le service est à l'arrêt.
        - Si l'un des deux rencontre une erreur critique, le service est détérioré.
        - Si l'un des deux n'est pas respecté, le service est légèrement détérioré.
    - Condition d'alarme des quatre ressources
        - Niveau de gravité général des conditions d'alarme (mineur, majeur ou critique)

Il est également nécessaire de déterminer la manière dont les répercussions des services métier influent sur les utilisateurs, autrement dit, d'identifier les utilisateurs affectés lorsque le service métier est altéré et de définir le niveau de gravité correspondant. Un client qui ne peut accéder à votre site de vente en ligne en est extrêmement gêné. Par conséquent, c'est très probablement un utilisateur vital (très important).

Si vos utilisateurs internes ne peuvent pas accéder à un serveur Web interne qui n'est pas essentiel pour leurs tâches quotidiennes, attribuez un niveau de gravité bien moindre à ce problème. Répondez aux questions suivantes pour vérifier l'impact de notre processus métier :

- Pouvez-vous trier la liste des utilisateurs de serveur classés par ordre d'importance ?
- Pouvez-vous ensuite organiser ces utilisateurs ou clients par société, organisation, service ou rôle ?



Vous devez également tenir compte des services réseau. De manière plus générale, les services réseau tels que DNS, DHCP et le courrier électronique affectent le service métier. Vous pouvez configurer des tests de temps de réponse et utiliser un service pour surveiller les serveurs fournissant le service. Cependant, vous devez les traiter quelque peu différemment. D'autres services peuvent également dépendre de ces services. C'est pourquoi vous devez les créer en pensant aux réutilisations possibles et à la modularité. Un exemple de service DNS et DHCP est illustré ci-dessous :

- SUBSERVICE : DNS
    - Composants : serveurs DNS SERVER-DNS1 et SERVER-DNS2
        - Si les deux serveurs sont à l'arrêt, le service l'est aussi.
        - Si un serveur est à l'arrêt, le service est légèrement détérioré.
    - Tests de temps de réponse : test du temps de réponse DNS
        - Si le temps de réponse est dépassé, le service est légèrement détérioré.
    - Condition d'alarme des deux ressources
        - Niveau de gravité général des conditions d'alarme (mineur, majeur ou critique)

Création de modèles de service et de relations

Cette section présente les concepts et les techniques de modélisation de service. Avant de créer des modèles de service, vous devez comprendre quelques concepts clés.

Principaux concepts

- **Surveillance des ressources.** Chaque modèle de service surveille activement ses ressources afin de déterminer l'intégrité de son service. Les ressources du service sont des modèles SPECTRUM et presque tous les modèles peuvent constituer une ressource de service. Les ressources du service peuvent être composées de tests SPM ou de modèles de périphérique, d'interface, de processus et même d'autres modèles de service. Pour surveiller une ressource, le service observe les attributs spécifiques du modèle de ressource. Un modèle de service peut surveiller les attributs définis sur des nombres entiers. L'observation des valeurs d'attribut des ressources est appelée la surveillance des ressources.
- **Etat de fonctionnement du service.** Le fonctionnement du service est représenté par un petit ensemble de valeurs : actif, à l'arrêt, détérioré et légèrement détérioré. Chaque moniteur de ressources détermine l'état de fonctionnement des services associés en fonction des valeurs d'attribut des ressources. Une stratégie de fonctionnement de service s'applique tout particulièrement aux valeurs collectives d'attribut des ressources. Une stratégie est en fait une formule qui calcule une valeur de fonctionnement de service en fonction d'une ou de plusieurs valeurs d'attribut de ressource. La logique appliquée par la stratégie est encapsulée dans un ensemble de règles de stratégie. Chaque règle représente une instruction qui, lors de son évaluation, est définie par « vrai » ou « faux ». Lors de l'évaluation d'une stratégie, la première règle identifiée comme vraie ou satisfaite détermine l'état de fonctionnement du service relevé par le service ou le moniteur de ressources.



- **Cause première et répercussions sur le service**. Etant donné qu'un service détermine son état de fonctionnement en surveillant ses ressources, il existe une relation logique entre les interruptions de ressources et l'état de fonctionnement du service. Cette relation s'exprime en termes de cause première et de répercussions sur le service. Lorsqu'une interruption de ressource modifie l'état de fonctionnement d'un service, elle constitue la cause première de cette modification. De la même manière, lorsqu'une interruption de ressource affecte le fonctionnement du service, elle influe sur ce dernier. Ces concepts deviennent essentiels pour les utilisateurs qui doivent faire face à des interruptions de service.
- **Modélisation hiérarchique de service.** Comme mentionné ci-dessus, chaque service est un moniteur de ressources qui détermine son état de fonctionnement en appliquant une stratégie à un ensemble de valeurs d'attribut de ses ressources. Il est important de noter qu'un service peut surveiller des ressources qui sont en fait d'autres services, ce qui permet de créer des hiérarchies de services ; un utilisateur peut ainsi créer des services avec des composants d'autres services. La modélisation de service sert alors à passer de modèles de services fondamentaux de bas niveau à des modèles de service conceptuels de haut niveau.

Création de modèles de service

Le processus de création d'un modèle de service comporte deux étapes principales :

1. Sélectionnez des ressources.

2. Sélectionnez la stratégie qui surveille les ressources.

Les exemples suivants illustrent la création de modèles de service représentant un service Web. Pour plus d'informations sur la création de modèles de service, reportez-vous au manuel *Service Manager User Guide*.

Exemple 1 : service d'accès au compte client

La détermination des ressources d'un service particulier peut sembler déconcertante. Dans de nombreux cas, vous ne pourrez pas considérer tous les composants possibles d'un service ni les associer en fonction de l'impact de chacun d'entre eux sur un service donné. Toutefois, SPECTRUM Service Manager offre un avantage fort utile : vous pouvez commencer par de petits modèles simples et les affiner progressivement à mesure que vous approfondissez vos connaissances des composants du service et des répercussions de chacun sur l'ensemble du service.

Même s'il s'avère difficile de connaître tous les composants d'un service, il est souvent facile d'identifier certains composants vitaux, ce qui constitue un bon point de départ. Prenons l'exemple d'un service Web simple, utilisé par un centre d'assistance téléphonique pour accéder aux données de compte client, et désigné comme le service d'accès au compte client.



Cette description générale de base suffit pour commencer à identifier certains composants du service. Puisqu'il s'agit d'un service Web, il doit être pris en charge par un ou plusieurs serveurs Web. De plus, le service fournit un accès aux informations depuis une base de données de comptes clients, probablement hébergée sur un ou plusieurs systèmes.
Dans cet exemple, supposons que l'environnement intègre deux serveurs Web et deux serveurs de base de données. Cela fournit un bon point de départ pour la modélisation du service. Si les deux serveurs Web ou les deux serveurs de base de données sont à l'arrêt, l'ensemble du service ne fonctionnera pas ; tant qu'un serveur Web ou de base de données est actif, le service fonctionne, même s'il est probable qu'il connaisse quelques dégradations. Cette description très simple fournit la base de la création du service d'accès au compte client.

- Pour commencer la modélisation des périphériques dans SPECTRUM, considérez chaque hôte de serveur Web et de base de données comme un modèle de ressources. La surveillance de l'état du contact de ces modèles de périphériques détermine si les systèmes sont actifs. Comme mentionné dans la section Principaux concepts, chaque service est un moniteur de ressources.
- SPECTRUM offre une formule de base pour le fonctionnement du service qui permet de connaître la disponibilité de ces quatre ressources de service. Le tableau suivant présente une matrice contenant chaque composant ainsi que la répercussion de l'état associé (actif/à l'arrêt) sur le service par rapport à l'état des autres ressources.



Tableau matriciel sur l'état de fonctionnement du service

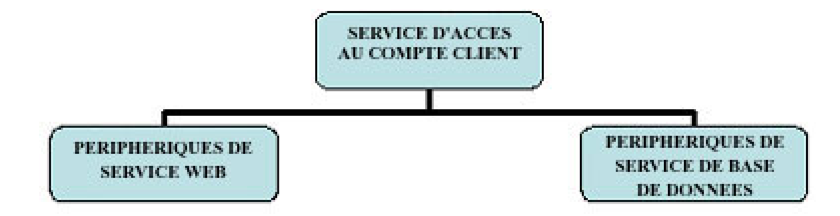
Serveur Web 1	Serveur Web 2	Serveur de base de données 1	Serveur de base de données 2	Service
ETABLI	ETABLI	ETABLI	ETABLI	ACTIF
PERDU	ETABLI	ETABLI	ETABLI	LEGEREMENT DETERIORE
ETABLI	PERDU	ETABLI	ETABLI	LEGEREMENT DETERIORE
ETABLI	ETABLI	PERDU	ETABLI	LEGEREMENT DETERIORE
ETABLI	ETABLI	ETABLI	PERDU	LEGEREMENT DETERIORE
PERDU	ETABLI	PERDU	ETABLI	DETERIORE
PERDU	ETABLI	ETABLI	PERDU	DETERIORE
ETABLI	PERDU	PERDU	ETABLI	DETERIORE
ETABLI	PERDU	ETABLI	PERDU	DETERIORE
PERDU	PERDU	ETABLI	ETABLI	ARRETE
PERDU	ETABLI	PERDU	PERDU	ARRETE
ETABLI	PERDU	PERDU	PERDU	ARRETE
ETABLI	ETABLI	PERDU	PERDU	ARRETE
PERDU	PERDU	PERDU	PERDU	ARRETE

Ce tableau indique que si les deux serveurs Web ou de base de données sont à l'arrêt, le service l'est aussi. Si un serveur Web et un serveur de base de données sont à l'arrêt, le service est détérioré. Si l'un des serveurs est à l'arrêt, le service est légèrement détérioré. Cette approche est très simplifiée mais elle constitue un bon point de départ.

A partir de là, vous pouvez étudier les modalités de surveillance de chaque composant. Le tableau montre que des combinaisons particulières de valeurs d'état entraînent des niveaux spécifiques de dégradation du service. En fait, vous pouvez classer les ressources en composants de serveur Web et en composants de base de données et considérer les ressources groupées comme des services au sein d'un service. Pour permettre l'activation du service d'accès au compte client, les composants des serveurs Web et de base de données doivent fonctionner. D'autres sous-services, plus discrets, peuvent exister au sein du service d'accès au compte client.



Si l'on considère que chaque service est également un moniteur de ressources, cet exemple illustre correctement la création de moniteurs de ressources au sein du service d'accès au compte client, comme indiqué ci-dessous.



Les moniteurs de ressources vous permettent d'organiser les ressources et de les surveiller en fonction de critères spécifiques en sachant quelles en seront les répercussions sur le service. Le moniteur de ressources devient une abstraction de plusieurs ressources et signale une valeur de fonctionnement en fonction de l'état collectif des ressources qu'il surveille. Ceci constitue la base d'une stratégie de surveillance des ressources d'un service.

Dans cet exemple, nous avons établi que vous pouvez surveiller l'état du contact de chaque modèle de périphérique pour déterminer sa disponibilité. De plus, le tableau présente les répercussions des différentes combinaisons de valeurs d'état de contact sur le service.
Si l'on regarde d'abord les serveurs Web, une stratégie peut être conduite pour indiquer correctement l'état des composants de serveur Web dans son ensemble. Ces instructions forment la stratégie de redondance des serveurs Web.

STRATÉGIE DE REDONDANCE DES SERVEURS WEB

- Lorsque le contact (statut) est perdu avec tous les serveurs Web, le composant serveur Web du service est à l'arrêt.
- Lorsque le contact (statut) est perdu avec l'un des serveurs Web, le composant serveur Web du service est détérioré.

Les composants Web et de base de données sont décrits comme des services au sein d'un service. Ce concept est important lorsque l'on travaille sur des groupes de ressources qui prennent en charge un aspect spécifique d'un service. Dans tous les cas, si les deux serveurs Web sont à l'arrêt, le service d'accès au compte client l'est aussi. Cependant, l'arrêt d'un seul serveur Web ne signifie pas nécessairement que le service d'accès au compte client est à l'arrêt ou détérioré. Vous pouvez considérer les serveurs Web, collectivement, comme un composant du service car lorsque l'un de ces serveurs est à l'arrêt, ce composant du service est détérioré. Cette approche peut sembler encore confuse, mais elle paraîtra plus évidente au fur et à mesure de l'évolution du modèle de service.

L'impact de la perte de contact avec les serveurs de base de données est le même que pour les serveurs Web. Ces instructions forment la stratégie de redondance des serveurs de base de données.

STRATÉGIE DE REDONDANCE DES SERVEURS DE BASE DE DONNÉES

- Lorsque le contact est perdu avec tous les serveurs de base de données, le composant base de données du service est à l'arrêt.
- Lorsque le contact est perdu avec l'un des serveurs de base de données, le composant base de données du service est détérioré.



Les serveurs Web et de base de données ont été décrits respectivement comme un composant de serveur Web et un composant de base de données. Etudiez les répercussions de ces composants sur le service d'accès au compte client.

Si les deux serveurs Web ou de base de données sont à l'arrêt, il en va de même pour le service. Ceux-ci étaient organisés en deux groupes : un composant de serveur Web et un composant de base de données, respectivement intitulés le moniteur de ressources des serveurs Web et le moniteur de ressources des serveurs de base de données. En résumé, chaque moniteur de ressources détermine sa propre valeur de fonctionnement, en fonction des ressources qu'il surveille. Le moniteur de ressources des serveurs Web détermine son propre état de fonctionnement à partir de l'état de contact des serveurs Web 1 et 2. Le moniteur de ressources des serveurs de base de données détermine son état de fonctionnement à partir de l'état de contact des serveurs de base de données 1 et 2.

L'encapsulation des systèmes de serveur Web et de serveur de base de données dans des moniteurs de ressources tient compte de ces instructions, qui forment la stratégie standard d'accès au compte.

STRATÉGIE STANDARD D'ACCÈS AU COMPTE

- Lorsque l'un des moniteurs de ressources est à l'arrêt, il en va de même pour le service d'accès au compte client.
- Lorsque tous les moniteurs de ressources sont détériorés, le service d'accès au compte client est détérioré.
- Lorsque l'un des moniteurs de ressources est détérioré, le service d'accès au compte client est légèrement détérioré.

Même s'il existe une certaine redondance dans chaque moniteur de ressources, si l'un des moniteurs est à l'arrêt, l'ensemble du service est à l'arrêt. Vous pouvez valider cette conception en consultant le tableau des valeurs d'état de contact et de fonctionnement des services. Pour tester la conception, vous pouvez utiliser les trois scénarios suivants.

SCÉNARIOS DE TEST DE LA CONCEPTION

- Le serveur Web 1 est à l'arrêt. Le moniteur de ressources du serveur Web se détériore ; les serveurs de base de données ne sont pas affectés, donc leur moniteur de ressources est actif. Pour appliquer les règles définies dans la stratégie d'accès au compte :
    - La première règle n'est pas remplie car aucun moniteur de ressources n'est à l'arrêt.
    - La deuxième règle n'est pas satisfaite car le moniteur de ressources de serveur de base de données est actif, et non détérioré.
    - La troisième règle, cependant, est satisfaite, car le moniteur de ressources de serveur Web est détérioré.

  Dans ce scénario, le service d'accès au compte client renvoie un état légèrement détérioré. Si vous consultez à nouveau la matrice, vous voyez que lorsque le serveur Web 1 est à l'arrêt et que tous les autres périphériques sont actifs, le fonctionnement général du service doit être considéré comme légèrement détérioré. La conception est tout à fait compatible avec ce scénario.



- Le serveur Web 1 et le serveur de base de données 1 sont à l'arrêt. D'après l'implémentation décrite ci-dessus, les deux moniteurs de ressources (serveur Web et serveur de base de données) doivent se détériorer. Lors de l'évaluation de la stratégie d'accès au compte, vous constatez que la deuxième règle est satisfaite et le service d'accès au compte client est détérioré. D'après la matrice, lorsque le serveur Web 1 et le serveur de base de données 1 sont tous les deux à l'arrêt, le fonctionnement général du service doit être dégradé, donc là encore, cette conception est correcte.
- Les serveurs de base de données 1 et 2 sont à l'arrêt. Dans ce cas, le moniteur de ressources du serveur de base de données est à l'arrêt. D'après la stratégie d'accès au compte, la première règle est satisfaite ; par conséquent, le service se met à l'arrêt. D'après la matrice, lorsque les serveurs de base de données 1 et 2 sont en panne, le service global doit l'être aussi.

Bien que ce soit un exemple très simple, ce processus a identifié les ressources d'un service et la manière de les surveiller. En dépit de sa simplicité, cette implémentation offre les connaissances permettant de générer correctement des rapports relatifs au fonctionnement du service d'accès au compte client pour 13 scénarios de défaillances différents impliquant les systèmes qui hébergent les applications du serveur de bases de données et des serveurs Web. A l'évidence, cette implémentation n'est pas encore très fiable car elle surveille uniquement l'état actif ou inactif des quatre systèmes. Avant d'étendre le service d'accès au compte client, consultez la procédure suivante pour implémenter cette conception à l'aide de SPECTRUM Service Manager.

MISE EN OEUVRE DE L'EXEMPLE 1 DANS SPECTRUM

Créez des modèles de service dans SPECTRUM à l'aide de l'éditeur Service Editor, que vous lancez à partir du menu Tools, Utilities de la console OneClick.

Pour commencer à créer le modèle de service :

1. Dans la console OneClick, sélectionnez Tools, Utilities, Service Editor.
2. Cliquez sur Create.
3. Spécifiez le nom de la stratégie Web Server Contact Monitor (moniteur de contact du serveur Web), ainsi qu'une description et une chaîne de sécurité.
4. Cliquez sur le bouton Locate resources and containers (jumelles).
5. Dans le volet gauche de la boîte de dialogue Locate Resources, cliquez sur Devices, Devices, By Model Name (ou By IP Address). Lancez la recherche sélectionnée (jumelles). Spécifiez les critères de recherche (les caractères génériques de début et de fin sont implicites pour le nom de modèle) et cliquez sur OK.
6. Dans le volet droit, sélectionnez tous les modèles de serveurs à associer à ce modèle de service.
7. Cliquez sur Add Selected to Monitored Resources.
8. Cliquez sur Close.
9. Cliquez sur Select pour afficher la boîte de dialogue Select Policy. Le moniteur de ressources utilise la stratégie de redondance des serveurs Web décrite précédemment dans ce chapitre.



10. Dans le volet gauche, définissez Value Map sur Contact Status.
11. Cliquez sur New dans l'ensemble de règles et nommez-le Web Server Redundancy Rules (règles de redondance du serveur Web).
12. Pour créer la première règle, cliquez sur Add : Rule Type All, When all are Down, the service is Down (Tous types de règles, lorsqu'elles sont toutes à l'arrêt, le service l'est aussi).
13. Cliquez sur OK.
14. Pour créer la deuxième règle, cliquez sur Add : Rule Type Any, When any 1 are Down, the service is Degraded (Tout type de règle, lorsque l'une d'entre elles est à l'arrêt, le service est détérioré).
15. Cliquez sur OK.
16. Dans la boîte de dialogue Create Rule Set, cliquez sur Create.
17. Cliquez sur OK.
18. Dans la boîte de dialogue Create Service, cliquez sur Create.
19. Pour démarrer la création du moniteur de contact du serveur de bases de données, répétez les étapes 2 à 10.

Remarque : Cette stratégie est identique aux règles de redondance des serveurs Web.

20. Dans le volet droit, sélectionnez Web Servers Redundancy Rule et cliquez sur Copy.
21. Définissez les nouveaux noms de règles sur Database Server Redundancy Rules.
22. Cliquez sur Create.
23. Pour fermer la boîte de dialogue Select Policy, cliquez sur OK.
24. Dans la boîte de dialogue Create Service, cliquez sur Create.
25. Cliquez sur Create pour démarrer la création du premier service (service d'accès au compte client) de la structure hiérarchique.
26. Spécifiez le nom du service d'accès au compte client et, le cas échéant, une description et une chaîne de sécurité.
27. Cliquez sur les jumelles, puis sur Locater, Services, Services, All. Lancez la recherche sélectionnée (jumelles).
28. Sélectionnez le paysage, le cas échéant.
29. Sélectionnez les services Web Server Contact Monitor et Database Server Contact Monitor.
30. Cliquez sur Add Selected to Monitored Resources.
31. Cliquez sur Close.



32. Cliquez sur Select pour afficher la boîte de dialogue Select Policy.

33. Dans le volet gauche, définissez Value Map sur Service Health.

34. Dans l'ensemble de règles, cliquez sur New et nommez-le Standard Account Access Policy, en fonction de l'ensemble de règles suivant :

    - Rule Type Any : When any 1 are Down, the service is Down (Tout type de règle, lorsque l'une d'entre elles est à l'arrêt, le service l'est aussi).
    - Rule Type All : When all are Degraded, the service is Degraded (Tous types de règles, lorsqu'elles sont toutes détériorées, le service l'est aussi).
    - Rule Type Any : When any 1 are Degraded, the service is Slightly Degraded (Tout type de règle, lorsque l'une d'entre elles est détériorée, le service est légèrement détérioré).

35. Dans la boîte de dialogue Rule Set, cliquez sur Create.

36. Cliquez sur OK.

37. Dans la boîte de dialogue Create Service, cliquez sur Create.

38. Fermez la fenêtre.

ANALYSE DE L'EXEMPLE 1

La conception de l'exemple 1 comprend un service qui surveille deux moniteurs de ressources. Dans cette approche à deux niveaux, chaque moniteur de ressources consolide l'état de ses propres ressources, puis consigne les résultats dans un rapport représentant le fonctionnement de son service. Le service d'accès au compte client détermine ensuite le fonctionnement de son propre service selon le fonctionnement collectif du service des deux moniteurs de ressources. Ce modèle englobe une abstraction importante essentielle à la compréhension de la gestion des services.

Chaque moniteur de services et de ressources exécute deux tâches :

- Il surveille les ressources auxquelles il est associé.
- Il détermine le fonctionnement de son propre service en appliquant à une stratégie des valeurs provenant de ces ressources.

Prenez connaissance des questions suivantes relatives à l'implémentation de l'exemple 1 :

- Le service d'accès au compte client a-t-il connaissance du serveur de base de données 2 ?

Les trois scénarios tests ne mentionnent pas la surveillance du serveur de base de données 2 par le service d'accès au compte client. Cependant, dans le scénario 3, lorsque les serveurs de base de données 1 et 2 sont tous deux à l'arrêt, le service d'accès au compte client a correctement déterminé que le fonctionnement de son service devait l'être aussi.



■ Comment fonctionne-t-il ?

Le moniteur de ressources des serveurs de base de données a déterminé que son fonctionnement était à l'arrêt. Le service d'accès au compte client, qui surveille les moniteurs de ressources des serveurs Web et de ressources des serveurs de bases de données, a déterminé que ces derniers devaient également être à l'arrêt. En évaluant sa stratégie d'accès au compte, il a remarqué que l'un des moniteurs de ressources était à l'arrêt et que, par conséquent, son propre fonctionnement devait l'être aussi. Les serveurs de base de données 1 et 2 sont des ressources du moniteur de ressources des serveurs de base de données, ce dernier étant une ressource du service d'accès au compte client. Chaque composant détermine son propre fonctionnement en fonction de ses ressources.

Exemple 2 : extension du service pour surveiller les processus vitaux

L'exemple 1 décrit la conception et l'implémentation d'un service très simple à l'aide de deux moniteurs de ressources. Bien que ce service soit légitime, il n'est pas très complet. En étudiant de nouveau le service d'accès au compte client, vous pouvez étendre la surveillance des composants de service de plusieurs manières. Jusqu'ici, seul l'état de contact des périphériques hébergeant les serveurs Web et de base de données a été incorporé au service. La seule disponibilité du périphérique ne garantit pas l'obtention des informations du compte client.

Vous devez également tenir compte du fait qu'un serveur Web est une application qui prend en charge les transactions Web. Pour que les demandes d'accès au compte client soient traitées, cette application doit être exécutée. En tenant compte de l'importance de ces systèmes de serveurs Web, il est logique qu'ils hébergent également un agent prenant en charge la surveillance des processus ou une MIB d'informations hôte telles que définie par les RFC 2790. Ceci permet à l'utilisateur de surveiller réellement le processus du serveur Web lui-même.

Vous pouvez utiliser un modèle de processus pour déterminer si un processus spécifique est réellement en cours d'exécution sur un périphérique. En tenant compte du fait que le système de serveurs Web peut être actif, mais que l'application du serveur Web peut être inactive, une surveillance supplémentaire des processus de l'application du serveur Web est importante pour déterminer correctement le fonctionnement global du service d'accès au compte client.

Dans un premier temps, il peut paraître assez simple d'ajouter simplement un autre moniteur de ressources pour observer la condition du modèle de processus du serveur Web et de traiter la disponibilité de chaque processus régulièrement, de la même façon que la disponibilité du périphérique est surveillée. Etudiez le tableau ci-dessous, qui décompose les scénarios de défaillances possibles et décrit l'effet de chaque combinaison sur la disponibilité des serveurs Web en termes de capacité à traiter une requête.
Ce tableau représente ce que l'on appelle souvent une « stratégie à haute sensibilité ».



Matrice de fonctionnement du service : serveurs et processus

Serveur Web 1	Serveur Web 2	Processus 1	Processus 2	Fonctionnement du service Web
ETABLI	ETABLI	NORMAL	NORMAL	ACTIF
ETABLI	ETABLI	VITAL	NORMAL	DETERIORE
ETABLI	ETABLI	NORMAL	VITAL	DETERIORE
ETABLI	ETABLI	VITAL	VITAL	ARRETE
PERDU	ETABLI	VITAL	NORMAL	DETERIORE
PERDU	ETABLI	VITAL	VITAL	ARRETE
PERDU	PERDU	VITAL	VITAL	ARRETE

Le tableau ci-dessous remplace chaque périphérique et processus par les moniteurs de ressources qui peuvent servir à les surveiller.

Matrice de fonctionnement du service : périphériques et processus

PERIPHERIQUES DE SERVEUR	PROCESSUS DE SERVEUR	SERVICE WEB
ACTIF	ACTIF	ACTIF
ACTIF	DETERIORE	DETERIORE
ACTIF	ARRETE	ARRETE
DETERIORE	DETERIORE	DETERIORE
DETERIORE	ARRETE	ARRETE
ARRETE	ARRETE	ARRETE
DETERIORE	ACTIF	DETERIORE
ARRETE	ACTIF	ARRETE
ARRETE	DETERIORE	ARRETE

Remarque : Les trois dernières lignes du tableau ne doivent généralement pas se produire puisqu'un système indiqué comme arrêté ne doit pas avoir de processus en exécution. Cependant, les règles doivent traiter ces situations pour éviter d'aboutir à des états inconnus.

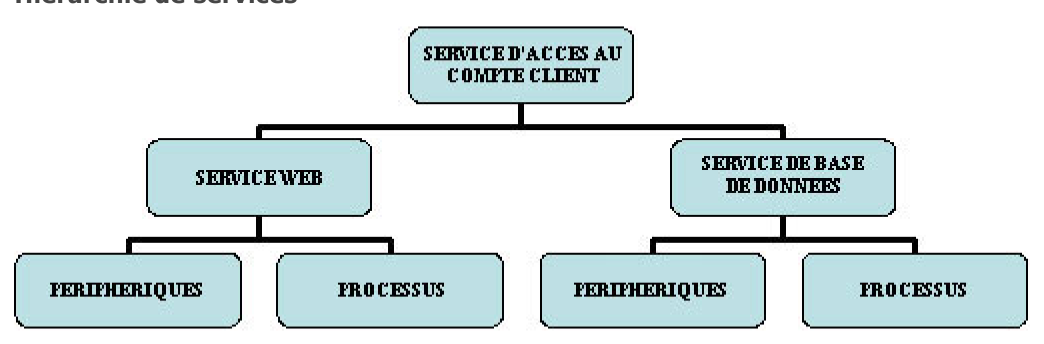


Si vous considérez les périphériques et les processus de manière conjointe, le tableau indique qu'une stratégie de redondance est inutile, ce qui semblait être la première possibilité lors de l'évaluation des ressources. Comme pour le service global, la relation entre les hôtes du service Web et les processus du serveur Web implique une règle à haute sensibilité similaire à celle-ci.

- Lorsqu'une ressource est à l'arrêt, le service l'est aussi.
- Lorsqu'une ressource est détériorée, le service l'est aussi.

Après évaluation de la relation entre les périphériques et les processus du serveur, il semble que vous ne puissiez pas étendre facilement la conception dans l'exemple 1 pour inclure une surveillance supplémentaire telle que l'ajout des nouveaux modèles de ressources du processus. Parce que la conception initiale essayait d'intégrer un service de haut niveau dans plusieurs composants, elle n'a pas reconnu l'existence de sous-services au sein du service d'accès au compte client. Après avoir étendu la surveillance au niveau du processus, il est clair qu'il existe un sous-service Web et un sous-service de base de données. De même que pour les serveurs Web, vous pouvez surveiller l'application hôte du service de base de données à l'aide de modèles de processus. La surveillance des ressources étant étendue au niveau du processus, une hiérarchie commence à apparaître.

Hiérarchie de services



Il n'est pas rare de découvrir des services de niveau inférieur qui, au départ, n'étaient pas assez significatifs pour engendrer un modèle de service. En général, le processus de modélisation de service est un processus itératif. Chaque révision ajoute des précisions et augmente le nombre total de scénarios de défaillance pouvant être rapportés correctement.

Cette approche itérative peut être résumée de différentes manières. L'une de ces manières consiste à considérer que le but de chaque révision est d'enrichir les informations sur la cause première qui seront disponibles en cas de défaillance du service. Reprenons l'exemple 1 : si les deux périphériques du serveur Web étaient disponibles, mais qu'un processus du serveur Web était à l'arrêt, le service n'aurait pas signalé de défaillance. Cependant, les utilisateurs du service auraient remarqué des détériorations des performances. En étendant la surveillance au niveau du processus, le service signale les détériorations et les échecs du processus comme cause première. La section suivante indique comment implémenter l'exemple 2 dans SPECTRUM.



Implémentation de l'exemple 2 dans SPECTRUM

La conception de l'exemple 2 comprend la création de quatre modèles de processus. Deux de ces modèles de processus surveillent l'application du serveur Web. Les deux autres surveillent l'application du serveur de base de données. Il est probable qu'un utilisateur identifie des processus supplémentaires ayant des conséquences sur la disponibilité d'un composant de service spécifique. Cette approche peut également être étendue pour inclure ces processus.

Pour créer les modèles de processus, vous devez localiser le modèle hôte représentant l'ordinateur serveur sur lequel le processus est exécuté. Dans l'exemple, il s'agirait d'un modèle de périphérique de serveur Web ou de serveur de base de données. Si l'agent du périphérique prend en charge RFC 2790, vous pouvez créer des modèles de processus pour chaque processus à surveiller.

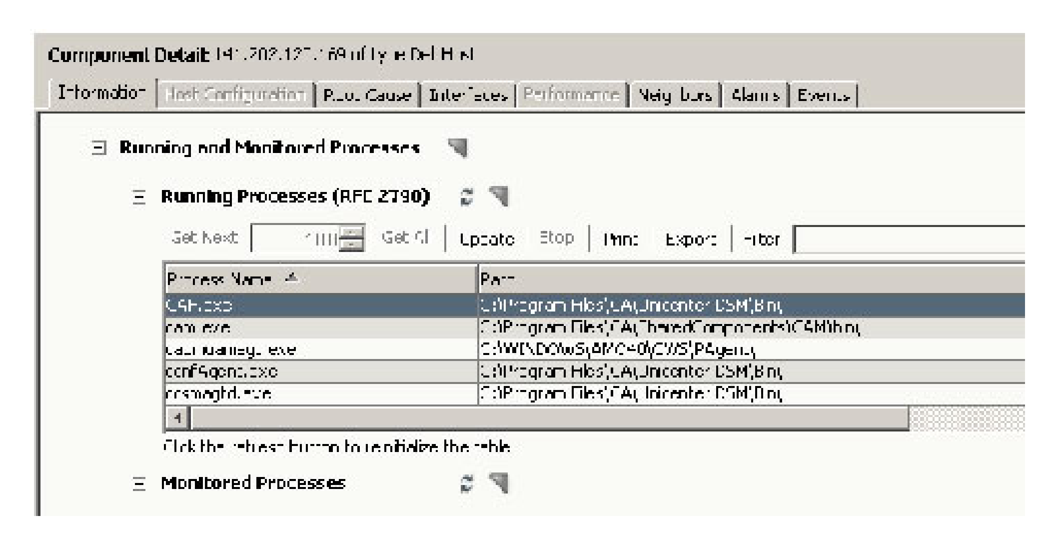
Pour créer un modèle de processus pour chaque processus :

1. Dans la console SPECTRUM OneClick, répertoriez les hôtes dans le panneau One Click Contents.

2. Sélectionnez l'hôte pour lequel vous souhaitez créer une règle de surveillance.

3. Dans la vue OneClick Component Detail, développez la section System Resources. Une sous-section appelée Running and Monitored Processes s'affiche.

4. Développez la vue Running and Monitored Processes pour afficher une section relative aux processus exécutés qui, à son tour, révèle un tableau de processus.



Remarque : Si le texte (RFC 2790) n'apparaît pas dans les noms de sections, l'agent ne prend pas en charge les extensions RFC 2790 vers MIB-II. Vous ne pourrez pas surveiller les processus sur cet hôte, ni déclencher des alarmes au démarrage et à l'arrêt des processus.

a. Cliquez avec le bouton droit de la souris dans le tableau et sélectionnez Monitor this process. La boîte de dialogue Add Monitored Process s'affiche.

b. Sélectionnez Alarm on Stop et cliquez sur OK. Grâce à ce paramètre, le modèle de processus déclenche une alarme critique en cas d'arrêt du processus correspondant. Le processus apparaît dans la vue Monitored Processes.



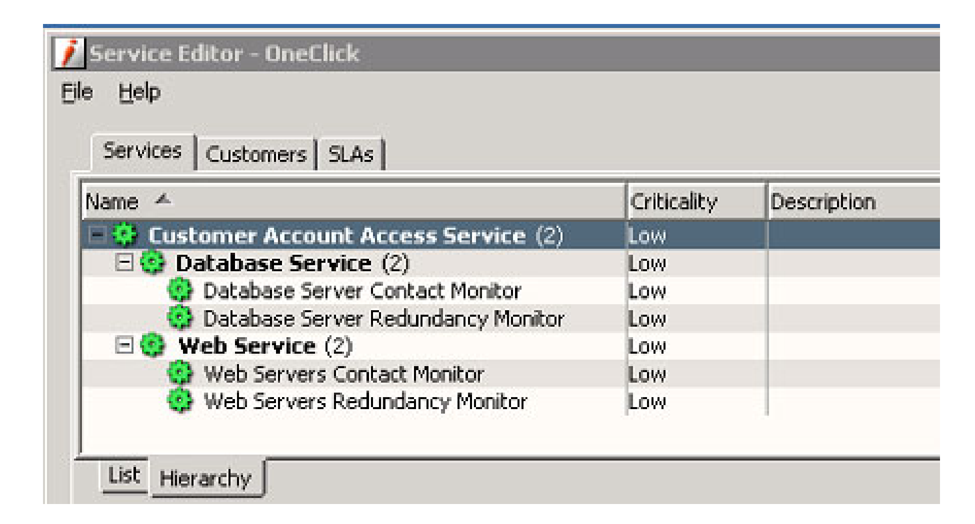
5. Après avoir créé les modèles de processus appropriés, lancez l'éditeur Service Editor en sélectionnant Tools, Utilities, Service Editor ou en cliquant avec le bouton droit de la souris sur un processus et en sélectionnant Utilities, Service Editor. Le but est de modifier le service créé dans l'exemple 1 et de traiter cette situation plus complexe à l'aide d'une procédure similaire à celle décrite pour l'exemple 1, mais avec une hiérarchie approfondie, en ajoutant une nouvelle couche intermédiaire et une logique relative aux processus.

    - A l'aide de la carte de valeurs de condition et de la stratégie de l'ensemble de règles de redondance, créez le service Web Servers Redundancy Monitor (moniteur de redondance des serveurs Web) qui observe les modèles de processus du serveur Web.
    - A l'aide de la stratégie Service Health High Sensitivity (haute sensibilité du fonctionnement du service), créez le service Web qui observe le moniteur de contact et celui de redondance des serveurs Web. Pour cela, vous devez rétablir la liaison du moniteur de contact des serveurs Web entre ce service et le service d'accès au compte client.
    - Répétez ces tâches pour le moniteur de redondance du serveur de base de données et le service de base de données.

    Le service d'accès au compte client va à présent surveiller le service Web et le service de base de données grâce à la stratégie standard d'accès au compte décrite dans la section relative à l'implémentation de l'exemple 1.

ANALYSE DE L'EXEMPLE 2

L'exemple 2 a étendu la plage de surveillance du service d'accès au compte client au processus du serveur Web réel. Cet exemple révèle également l'existence de deux sous-services distincts au sein du service d'accès au compte client. Chacun de ces sous-services est composé de plusieurs ressources surveillées de différentes manières, comme indiqué dans la vue Hierarchy de Service Editor ci-dessous.



Le tableau ci-dessous présente l'ensemble toujours grandissant de scénarios de défaillance pouvant être pris en charge par la modélisation de service existante.



Matrice avec scénarios de défaillances de service

Légende :

- **WSD :** périphérique du serveur Web
- **WSP :** processus du serveur Web
- **DBD :** périphérique de la base de données
- **DBP :** processus de la base de données
- **CAAS** : service d'accès au compte client
- **DG :** service détérioré
- **SD :** service légèrement détérioré
- **DN :** service à l'arrêt

WSD 1	WSD 2	WSP 1	WSP 2	DBD 1	DBD 2	DBP 1	DBP 2	CAAS
ACTIF	ACTIF	ACTIF	ACTIF	ACTIF	ACTIF	ACTIF	ACTIF	ACTIF
ACTIF	DN	ACTIF	DN	ACTIF	ACTIF	ACTIF	ACTIF	SD
DN	ACTIF	DN	ACTIF	ACTIF	ACTIF	ACTIF	ACTIF	SD
ACTIF	ACTIF	DN	ACTIF	ACTIF	ACTIF	ACTIF	ACTIF	SD
ACTIF	ACTIF	ACTIF	DN	ACTIF	ACTIF	ACTIF	ACTIF	SD
ACTIF	ACTIF	ACTIF	ACTIF	DN	ACTIF	DN	ACTIF	SD
ACTIF	ACTIF	ACTIF	ACTIF	ACTIF	DN	ACTIF	DN	SD
ACTIF	ACTIF	ACTIF	ACTIF	ACTIF	ACTIF	DN	ACTIF	SD
ACTIF	ACTIF	ACTIF	ACTIF	ACTIF	ACTIF	ACTIF	DN	SD
DN	ACTIF	DN	ACTIF	DN	ACTIF	DN	ACTIF	DG
DN	ACTIF	DN	ACTIF	ACTIF	DN	ACTIF	DN	DG
ACTIF	DN	ACTIF	DN	DN	ACTIF	DN	ACTIF	DG
ACTIF	DN	ACTIF	DN	ACTIF	DN	ACTIF	DN	DG
ACTIF	ACTIF	DN	ACTIF	ACTIF	ACTIF	DN	ACTIF	DG
ACTIF	ACTIF	DN	ACTIF	ACTIF	ACTIF	ACTIF	DN	DG
ACTIF	ACTIF	ACTIF	DN	ACTIF	ACTIF	DN	ACTIF	DG
ACTIF	ACTIF	ACTIF	DN	ACTIF	ACTIF	ACTIF	DN	DG
DN	DN	DN	DN	ACTIF	ACTIF	ACTIF	ACTIF	DN
DN	DN	DN	DN	DN	ACTIF	DN	ACTIF	DN



WSD 1	WSD 2	WSP 1	WSP 2	DBD 1	DBD 2	DBP 1	DBP 2	CAAS
DN	DN	DN	DN	ACTIF	DN	ACTIF	DN	DN
ACTIF	ACTIF	DN	DN	ACTIF	ACTIF	ACTIF	ACTIF	DN
ACTIF	ACTIF	DN	DN	DN	ACTIF	DN	ACTIF	DN
ACTIF	ACTIF	DN	DN	ACTIF	DN	ACTIF	DN	DN
ACTIF	ACTIF	DN	DN	ACTIF	ACTIF	DN	ACTIF	DN
ACTIF	ACTIF	DN	DN	ACTIF	ACTIF	DN	DN	DN
DN	DN	DN	DN	DN	DN	DN	DN	DN

Le tableau indique 25 scénarios de défaillance différents pouvant être signalés grâce à l'implémentation de l'exemple 2. Notez que le scénario indiqué dans la ligne ci-dessus est en gras. Dans ce scénario, tous les processus vitaux ont échoué. Dans ce cas, le service est arrêté. Cette information n'aurait pas été signalée si vous aviez implémenté l'exemple 1.

Exemple 3 : extension du service pour inclure un élément de temps de réponse

L'exemple 2 a amélioré le service d'accès au compte client en étendant la visibilité au niveau du processus. Dans certains cas, les périphériques peuvent être actifs et les processus en exécution, mais le service ne fonctionne pas de façon optimale. Il est parfois utile d'inclure une surveillance des performances comme ressource des composants de service. Ceci est particulièrement important lorsque le fonctionnement du service a pour but de refléter les différentes étapes suivies par l'utilisateur final lorsqu'il utilise un service.

Dans cet exemple, vous ajoutez un élément de temps de réponse au composant du service Web du service d'accès au compte client. L'ajout de l'élément de performances permet non seulement d'améliorer la surveillance du service, mais aussi de tester la modularité de la conception produite dans l'exemple 2. L'un des objectifs de la conception des services doit consister à produire des services faciles à améliorer à mesure que vous approfondissez vos connaissances de la surveillance de chaque ressource de service.

L'ajout du composant de temps de réponse implique la création de modèles de tests du temps de réponse dans SPECTRUM. Bon nombre de périphériques et d'agents système peuvent prendre en charge des tests du temps de réponse. Puisque cet exemple a pour but d'améliorer la surveillance du composant de service Web, vous allez créer des tests de temps de réponse HTTP.

Le nombre de tests peut varier selon votre conception. Généralement, il est préférable de créer au moins une requête HTTP pour chaque serveur Web. Par exemple, vous pouvez sélectionner deux hôtes de test SPM et créer deux tests HTTP sur chacun d'eux. L'hôte de test doit émettre des requêtes pour chaque serveur Web. Ceci fournit plusieurs points de requêtes pour chaque serveur. Les quatre nouveaux tests de temps de réponse comprennent collectivement un nouvel ensemble de ressources au sein du service Web.



Vous pouvez utiliser deux approches standard pour surveiller les tests du temps de réponse :

- Surveiller le dernier état d'erreur de chaque modèle de test du temps de réponse.
- Surveiller l'ensemble des valeurs de résultats de chaque modèle de test.

La seconde approche est exposée en détail plus loin dans ce livre. Pour cet exemple, vous allez surveiller le dernier état d'erreur de chaque modèle de test. Le tableau ci-dessous établit une correspondance entre les valeurs du dernier état d'erreur (temps de réponse) et les valeurs de fonctionnement du service équivalentes. Ce processus est largement utilisé par SPECTRUM Service Manager. Le but est de normaliser les valeurs d'attribut pures par rapport à des valeurs de fonctionnement du service comparables pouvant être aisément appliquées à différents ensembles de règles.

Matrice de fonctionnement du service : tests de réponse

Valeur du temps de réponse	Fonctionnement du service équivalent
OK	ACTIF
DELAI D'ATTENTE	CRITIQUE
SEUIL CRITIQUE	CRITIQUE
SEUIL MAJEUR	DETERIORE
SEUIL MINEUR	LEGEREMENT DETERIORE

Dans certaines circonstances, la documentation peut indiquer des niveaux de temps de réponse acceptables. Dans le cas contraire, l'une des approches possibles consiste à créer des tests du temps de réponse sans seuil et à consulter les résultats de latence sur une période donnée. Ceci vous aide à établir des valeurs de seuil de référence pour garantir qu'une valeur de latence inhabituelle entraîne une violation du seuil.

Dans l'exemple 2, le service Web a été développé de manière à inclure un moniteur de ressources pour l'état de contact des périphériques du serveur Web et un moniteur de ressources pour la condition des modèles de processus du serveur Web. Il est possible d'étendre la surveillance du service Web de manière à inclure le composant de temps de réponse en ajoutant simplement un troisième moniteur de ressources qui surveille les modèles de tests du temps de réponse.

L'ensemble de règles suivant peut être approprié à la surveillance de ces modèles de tests du temps de réponse :

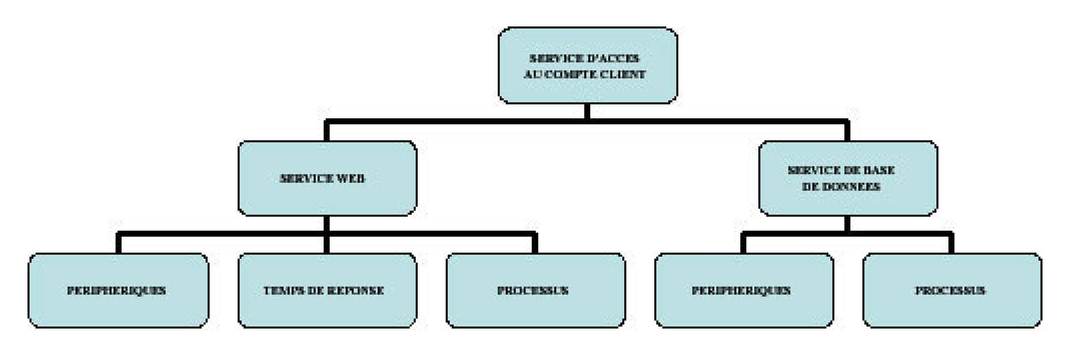
- Lorsque toutes les ressources sont arrêtées, le service l'est aussi.
- Lorsqu'une ressource est arrêtée, le service est détérioré.
- Lorsque toutes les ressources sont détériorées, le service l'est aussi.



Etudiez le mode d'application de ces règles sur un ensemble de tests du temps de réponse tel que décrit ci-dessus.

- Si tous les tests du temps de réponse ont subi un délai d'attente ou une violation de seuil critique, cela signifie qu'aucun serveur Web n'a pu répondre. Il s'agit clairement d'un scénario critique qui doit indiquer un arrêt de fonctionnement du service.
- Si un test du temps de réponse a rencontré un délai d'attente ou a dépassé un seuil critique, cela signifie que l'un des serveurs Web a été touché, à tel point qu'il n'a pu traiter les requêtes de manière adéquate. En tenant compte du fait que certains autres tests du temps de réponse sont effectués avec succès, on peut supposer que le service n'est pas complètement arrêté, mais qu'il est détérioré.
- Si aucun des tests n'a rencontré de délai d'attente ou n'a dépassé de seuil critique, mais qu'ils ont tous dépassé un seuil majeur, vous pouvez en déduire que le fonctionnement du service est détérioré.

En fonction de la configuration établie ci-dessus, vous pouvez améliorer le service Web en ajoutant un nouveau moniteur de ressources pour les tests du temps de réponse. Le composant de service Web fonctionne correctement dans tous les scénarios décrits ci-dessus. En surveillant ses ressources à l'aide de la stratégie de haute sensibilité du fonctionnement du service, chaque moniteur de ressources arrêté provoquerait l'arrêt du service Web. De même, chaque ressource détériorée provoquerait la dégradation du service Web. Il apparaît que la conception produite dans l'exemple 2 peut être aisément étendue de manière à inclure l'élément de temps de réponse. L'exemple ci-dessous illustre la hiérarchie de services après l'ajout du composant de temps de réponse au service Web.



IMPLÉMENTATION DE L'EXEMPLE 3 DANS SPECTRUM

Pour cet exemple, vous allez créer quatre tests du temps de réponse HTTP. Vous pouvez localiser les hôtes des tests du temps de réponse à l'aide de l'onglet Locator de la console OneClick. Le menu Locator intègre un ensemble de fonctions de recherche SPM préconfigurées.

Remarque : Pour exécuter un test HTTP, vous devez découvrir les sources de tests telles que les agents SystemEDGE Service Availability, les routeurs compatibles avec les contrats de niveau de service Cisco IP et les agents Network Harmoni, à l'aide de chaînes de communauté en lecture-écriture. Pour plus d'informations sur les tests de réponse et les agents pris en charge, reportez-vous au manuel *Service Performance Manager User Guide*.



Pour créer des tests du temps de réponse :

1. Utilisez la recherche All Test Host pour localiser les modèles d'hôtes de tests capables de mesurer le temps de réponse HTTP aux serveurs Web. Pour ce faire, dans le volet Contents, développez SPM Searches et Test Hosts By. Cliquez ensuite avec le bouton droit de la souris sur All Test Hosts et sélectionnez Launch the selected search.

2. A partir de chaque hôte de test désigné, créez des tests HTTP en cliquant avec le bouton droit de la souris sur l'hôte dans le tableau. Choisissez New Test et sélectionnez HTTP.

3. Spécifiez les données des seuils. Configurez les seuils de manière à garantir la génération d'un seuil critique en cas de temps de réponse trop lent pour être utilisé et la génération d'un seuil majeur lorsque le temps de réponse est utilisable, mais très lent. Ajoutez la destination du test, c'est-à-dire l'un des hôtes du serveur Web.

4. Pour ajouter les tests du temps de réponse, utilisez l'éditeur Service Editor pour ajouter le nouveau moniteur de ressources (Web Server Response Monitor, moniteur de réponses du serveur Web) qui utilise la stratégie Response Time High Sensitivity (haute-sensibilité du temps de réponse). Vous pouvez localiser les ressources en développant SPM Searches. Vous pouvez ensuite ajouter les quatre tests du temps de réponse au nouveau moniteur de ressources. Enfin, joignez cette nouvelle ressource au service Web.

ANALYSE DE L'EXEMPLE 3

L'exemple 3 vous indique comment étendre une implémentation de service existante pour inclure une surveillance des ressources plus sophistiquée sans modifier la hiérarchie de services. Cette souplesse de la hiérarchie de services permet aux utilisateurs d'améliorer continuellement et facilement leurs modèles de service. De plus, l'exemple 3 met en avant la méthode d'incorporation d'un composant du temps de réponse au sein d'un service de manière à améliorer considérablement la précision des rapports de fonctionnement du service. Encore une fois, cette itération a permis une prise en charge accrue des scénarios de défaillance et a enrichi l'ensemble de causes premières potentielles de l'impact sur les services.

Création de contrats de niveau de service

Cette section présente les concepts et techniques de la modélisation de contrats de niveau de service. Vous devez les comprendre avant de modéliser des contrats de niveau de service.

Remarque : Les sections suivantes, jusqu'à l'exemple 4 inclus, fournissent des instructions concernant le suivi des contrats de niveau de service en fonction des heures de fonctionnement. SPECTRUM Release 8.1 comprend cette fonctionnalité. Pour obtenir une description complète des capacités disponibles, reportez-vous au manuel *Service Performance Manager User Guide*.



Principaux concepts

- **Périodes des contrats de niveau de service.** Les contrats de niveau de service consistent en un ensemble d'objectifs et de garanties du niveau de service, mesurés sur une période donnée. Cette période correspond généralement à un cycle de facturation précis ou à un cycle de génération de rapports. Une période de contrat de niveau de service est souvent mensuelle (c'est-à-dire que le respect d'un contrat de niveau de service est évalué d'un mois à l'autre). Généralement, le respect ou le non respect d'un contrat de niveau de service est exprimé pour une période spécifique. Par exemple, vous pouvez considérer qu'un contrat de niveau de service est respecté pour le mois de janvier. Si la période est évaluée sur une base hebdomadaire, vous pouvez considérer qu'un contrat de niveau de service a été violé pour la semaine du 5 au 11 novembre.
- **Garanties de contrats de niveau de service ou objectifs de niveau de service.** Un contrat de niveau de service comprend, entre autres, un ensemble de garanties ou d'objectifs de niveau de service. En particulier, bon nombre de ces garanties portent sur la disponibilité et les performances d'un service ou d'un ensemble de services spécifiques. Dans les environnements de fourniture de services standard, les contrats de niveau de service établissent souvent des garanties très spécifiques. Les utilisateurs peuvent trouver des clauses de type : « ...certifie un temps de fonctionnement de 99,9 % par mois... » ou « ...créditera le client d'un trentième du prix du service mensuel s'il signale une interruption de 30 minutes ou plus... » Ces déclarations représentent les garanties données par le fournisseur par rapport à un service spécifique. Il existe également des contrats de niveau de service au sein de l'environnement d'entreprise, bien que plus informels. Il n'est pas rare de trouver des contrats de niveau de service comportant des clauses telles que « ...le service informatique garantit un temps d'arrêt de l'accès Internet inférieur à 30 minutes par semaine... » Dans tous les cas, ce sont ces garanties ou objectifs de niveau de service qui fournissent les bases permettant de déterminer la conformité du contrat de niveau de service à SPECTRUM.
- **Surveillance active du contrat de niveau de service.** A la différence d'autres produits de gestion des contrats de niveau de service, SPECTRUM Service Manager offre une gestion active de ces derniers. Ainsi, vous pouvez déterminer l'état du contrat de niveau de service sur une période donnée. Vous avez accès à un état prévu pour toute la période, selon les tendances d'interruption. Au début de chaque période de contrat de niveau de service, un contrat est considéré comme non affecté. Cet état est maintenu jusqu'à ce qu'une interruption provoque l'enregistrement d'un temps d'interruption pendant la période du contrat de niveau de service. L'état d'un contrat de niveau de service ayant enregistré un temps d'interruption, sans risque significatif de violation, est considéré conforme.

  Si d'autres temps d'interruption se produisent durant la période et que leur accumulation atteint des niveaux qui peuvent représenter un risque de violation du contrat de niveau de service, le contrat passera à un état d'avertissement. Si le temps d'interruption se poursuit et que les seuils de garantie spécifiques sont atteints, le contrat de niveau de service passera à un état de violation. Ce passage de l'état non affecté à l'état de violation s'effectue en temps réel. Si la période du contrat de niveau de service est mensuelle et que ce dernier est violé le cinquième jour, vous serez averti immédiatement, plutôt que d'attendre le rapport de fin de période notifiant la violation. Cette surveillance active des contrats de niveau de service permet ainsi aux fournisseurs de service d'agir avant la violation du contrat.



- **Heures de mise en application ou de fonctionnement des contrats de niveau de service.** Pendant la durée du contrat de niveau de service, une garantie spécifique est fréquemment mise en application. Le contrat de niveau de service peur contenir des clauses telles que « ...garantit l'absence d'interruption de plus de 30 minutes entre 8 heures et 17 heures du lundi au vendredi... » Une clause comme celle-ci est généralement appelée une garantie des heures de fonctionnement. Parfois, plusieurs garanties reposent sur des délais spécifiques. Par exemple, « ...garantit 97,5 % de disponibilité 7/7 jours, 24/24 heures, avec 99,9 % de disponibilité de 8 heures à 17 heures du lundi au vendredi et de 8 heures à 12 heures le samedi... » Bien qu'un seul service soit concerné, cette clause comprend réellement deux garanties : la première avec un délai d'exécution 7/7 jours et 24/24 heures, la deuxième pour des heures spécifiques de la semaine.

Création de contrats de niveau de service et de garanties

La première étape de la création d'un contrat de niveau de service consiste à comprendre le service spécifique avec lequel il est associé et la période de validité de ce contrat. La hiérarchie de modélisation des services comporte souvent des modèles de service supérieurs qui sont logiquement associés à un contrat de niveau de service. Par exemple, un environnement de fourniture de services peut inclure un service de haut niveau nommé Client A : données haute vitesse.

Logiquement, le contrat de niveau de service constitue une liaison du service de données haute vitesse proposé au client A. La période spécifique peut être stipulée dans un contrat de niveau de service ou déterminée de façon arbitraire, mais le fournisseur de service et le client du service doivent tous deux accepter ce délai. Les périodes mensuelles de contrats de niveau de service sont très courantes puisqu'elles coïncident souvent avec le cycle de facturation. Par exemple, une période de contrat de niveau de service peut prendre effet le premier jour du mois et comporter des garanties qui dépendent de la disponibilité et des performances au cours de ce mois. Généralement, un contrat de niveau de service spécifie des garanties de restitution au cas où un client contacterait le fournisseur de services suite à un litige survenu quelques jours après la fin d'une période donnée.

Une fois le service principal et la période du contrat de niveau de service déterminés, l'utilisateur doit identifier les garanties du contrat de niveau de service ou les objectifs du niveau de service relatifs à la disponibilité et aux performances du service fourni. Ces garanties se trouvent habituellement dans le document du contrat de niveau de service, parmi d'autres clauses ne portant pas sur la mesure de la disponibilité ou des performances d'un service. Nous vous conseillons de lire les déclarations qui spécifient un niveau de disponibilité, un temps de réponse garanti, un niveau acceptable de latence, etc. De plus, nous vous conseillons de vérifier si ces déclarations sont suivies d'autres indications sur des heures de garantie spécifiques pendant la durée du contrat de niveau de service.

Après avoir identifié les garanties d'un contrat de niveau de service, vous devez les classer en garanties de disponibilité ou de temps de réponse. Dans le contrat de niveau de service, les garanties de disponibilité sont souvent spécifiées sous la forme d'un pourcentage de disponibilité. Cependant, elles peuvent être décrites en termes de temps d'arrêt. Par exemple, « ...moins d'une heure d'interruption... » Les garanties de temps de réponse peuvent être identifiées par des déclarations telles que « ...temps de réponse de 2 000 ms ou plus... » ou « ...latence inférieure à 5 000 ms depuis plus de 30 minutes... »



La disponibilité peut être définie de plusieurs manières. Les sections précédentes de ce document ont présenté le fonctionnement du service. Généralement, vous pouvez décrire la disponibilité comme suit : un service est disponible lorsqu'il est en cours de fonctionnement ; un service est indisponible lorsqu'il est à l'arrêt. Cependant, une garantie de disponibilité peut également s'appliquer à un service indisponible dans la mesure où il n'est pas réactif. Cette seconde description peut s'avérer très importante lors de la création de modèles de garanties.

Le temps de réponse garantit une mesure des services utilisant les composants du temps de réponse comme ressources. Dans le cadre des garanties de temps de réponse, il est intéressant de remarquer que les composants d'une hiérarchie de services peuvent surveiller le temps de réponse dans le but précis d'assurer la prise en charge d'une garantie de temps de réponse dans le contrat de niveau de service. Ce scénario est même très fréquent.

La conception d'une hiérarchie de services repose très souvent sur les ressources qui comprennent réellement les périphériques physiques et des applications fournissant un service destiné aux utilisateurs. Bien qu'ils offrent un excellent moyen de générer des rapports sur le fonctionnement du service, les tests du temps de réponse sont souvent identifiés comme des ressources de service après l'application d'un contrat de niveau de service stipulant des garanties de temps de réponse. Comme indiqué dans les sections précédentes, vous pouvez utiliser des moniteurs de temps de réponse pour identifier une latence importante ou une détérioration du service. Les tests du temps de réponse doivent signaler une violation de seuil majeur lorsque la latence dépasse un niveau acceptable. De plus, vous pouvez également utiliser les moniteurs de temps de réponse pour signaler une condition critique lorsque la latence atteint un niveau inutilisable ou que le temps de réponse requiert un délai d'attente. Ainsi, les moniteurs de temps de réponse créés peuvent prendre en charge à la fois la notion de latence et de disponibilité de la surveillance.

Si un service est considéré comme indisponible lorsqu'il n'est pas réactif (bien que le temps de réponse d'un service conçu pour signaler la disponibilité ne fasse jamais l'objet d'une garantie), un service conçu pour indiquer le temps de réponse peut également servir à mesurer la disponibilité.

Exemple 4 : contrat de niveau de service pour le service d'accès au compte client

La présente section contient un exemple basé sur le service d'accès au compte client de la section précédente. Il comprend un contrat de niveau de service et plusieurs garanties.

Dans la section Création de modèles de service du présent chapitre, vous avez implémenté le service d'accès au compte client. Dans cet exemple, le service d'accès au compte client représente le service fourni par une entreprise fictive nommée Solutions de données du Nord (ci-après appelée SDN).

SDN gère les informations de comptes clients pour un grand nombre de petites entreprises. Chaque petite entreprise est responsable de la création et de la maintenance des données de ses clients. SDN assume la prise en charge et la sécurisation des données des comptes clients. Outre la prise en charge des bases de données et de l'accès Internet, SDN négocie avec différents fournisseurs de services Internet pour offrir un périphérique de routage local au site client distant et garantir aux clients un accès Internet fiable à leurs informations de compte client. Pour les clients de SDN, la relation avec le fournisseur de services Internet est transparente. Ils paient directement le service à SDN.



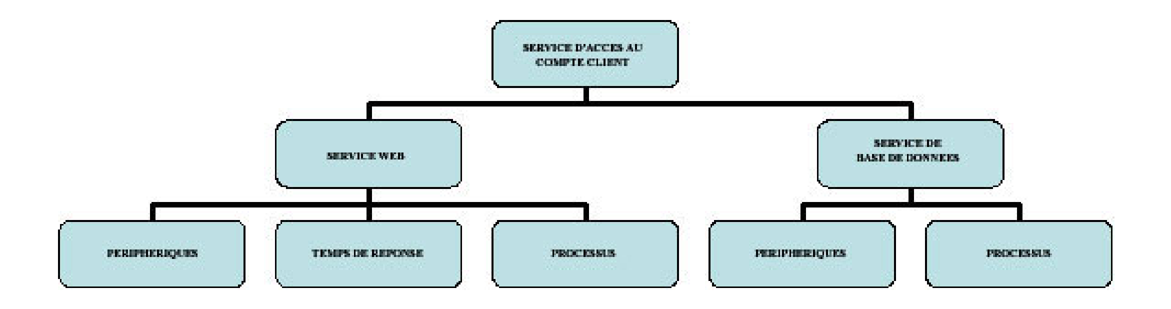
Les éléments suivants sont des extraits d'un contrat de niveau de service fourni à chaque client de SDN :

- SDN fournit un accès aux données des comptes clients en garantissant chaque mois un taux de disponibilité de 99 % sur chaque site client, en dehors des périodes de maintenance du système planifiées entre minuit et 3 heures du matin tous les dimanches.
- La disponibilité du service sera restaurée de manière à ce que le temps moyen de résolution des interruptions soit de 30 minutes maximum, sans interruption supérieure à 1 heure. Nous garantissons moins de deux interruptions par périodes de 24 heures.
- Une plage horaire de fonctionnement standard définie entre 7 heures et 18 heures (heure de la côte Est américaine) du lundi au vendredi, toutes les semaines.
- Pendant ces heures de fonctionnement standard, la disponibilité de l'accès aux comptes est garantie à 99,5 % sans interruption de plus de 20 minutes.
- Le temps de transaction moyen pour un accès initial aux comptes ne doit pas dépasser cinq secondes pour plus de 5 % de la plage horaire de fonctionnement standard, avec une exécution des transactions réussie garantie à 99 % pendant les heures de fonctionnement standard. Avec une transaction réputée réussie si elle est exécutée dans un délai de 15 secondes, aucun échec de transaction ne dure plus de 20 minutes.
- La moyenne de surveillance des transactions basée sur un échantillon de cinq requêtes à émettre de manière aléatoire dans un intervalle de cinq minutes pendant les heures de fonctionnement standard, chaque requête provenant du périphérique du point d'accès client.
- SDN assume la responsabilité d'un périphérique d'accès en supposant que le périphérique fonctionne, sauf dans le cas d'une panne d'alimentation ou d'un événement naturel dépassant les compétences de SDN.

Dans cet exemple, le texte du contrat de niveau de service comprend différentes mesures et différents termes de garantie permettant des déclarations fictives typiques telles que celles rencontrées dans un contrat de niveau de service réel. En dépit de sa terminologie déroutante, ce contrat de niveau de service contient des informations de garantie très précises, y compris concernant la mesure réelle du temps de réponse.

Ce contrat de niveau de service serait fourni à chaque client de SDN. Dans cet exemple, nous allons nous concentrer simplement sur celui qui lie SDN à un client appelé Composants de performances A à Z, dont les bureaux se situent à Paris et à Lille.

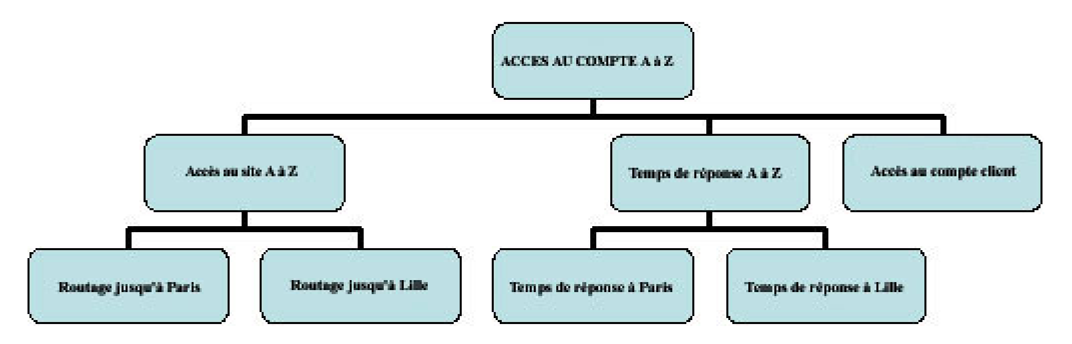
Comme indiqué ci-dessus, la première étape de la conception d'une implémentation de contrat de niveau de service consiste à déterminer le service qui prend en charge le contrat et à identifier la période. La hiérarchie ci-dessous représente le service d'accès au compte client.





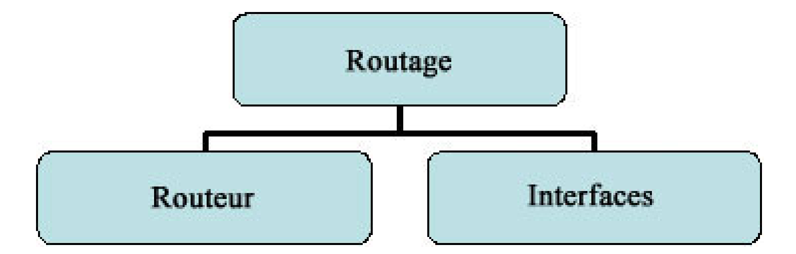
La surveillance de la disponibilité du service d'A à Z requiert de nombreux composants. En plus de fournir un accès Internet et aux bases de données, SDN doit à présent créer des composants de service qui surveillent la disponibilité et le temps de réponse spécifiques aux bureaux de Paris et de Lille d'A à Z.

Ces nouveaux composants de service vont surveiller les routeurs d'accès sur chaque site et le temps de réponse des nouveaux tests du temps de réponse hébergés par ces routeurs sur chaque site. L'illustration suivante indique comment étendre la hiérarchie de manière à prendre A à Z en charge.



L'évaluation du contrat de niveau de service implique qu'il existe différentes garanties et que des nouveaux modèles de services seront requis. Le tableau ci-dessus représente une configuration possible. Nous vous conseillons de consulter attentivement chaque implémentation de contrat de niveau de service pour déterminer le meilleur moyen d'organiser les services.

Une hiérarchie appelée Accès au site A à Z fait partie des nouveaux services. L'accès au site A à Z contient deux sous-services appelés Routage jusqu'à Paris et Routage jusqu'à Lille. Ces services sont conçus pour surveiller le routeur sur site fournissant l'accès au service d'accès au compte client. Vous pouvez décomposer chacun de ces sous-services en un ensemble de moniteurs de ressources, créant ainsi une hiérarchie semblable à l'illustration ci-dessous.





Un moniteur de ressources observe l'état de contact du modèle de périphérique du routeur, tandis que l'autre moniteur de ressources observe l'état du port des interfaces sur le routeur, vitales pour fournir un accès au bureau. Si le routeur est arrêté ou si toutes les interfaces requises sont désactivées, le service de routage est considéré comme arrêté. Un service similaire est implémenté pour Paris et Lille. En référence au contrat de niveau de service, les déclarations suivantes s'appliquent aux composants de routage de chaque site :

- SDN fournit un accès aux données des comptes clients en garantissant chaque mois un taux de disponibilité de 99 % sur chaque site client, en dehors des périodes de maintenance du système planifiées entre minuit et 3 heures du matin tous les dimanches.
- La disponibilité du service sera restaurée de manière à ce que le temps moyen de résolution des interruptions soit de 30 minutes maximum, sans interruption supérieure à 1 heure. Nous garantissons moins de deux interruptions par période de 24 heures.

Les garanties s'appliquent à chaque site. Considérons que vous offrez à l'utilisateur du gestionnaire de services 99 % de disponibilité pendant le mois de novembre. Un temps d'arrêt de 432 minutes est ainsi autorisé. Lors de la création du contrat de niveau de service, étudiez attentivement les services auxquels cela s'applique. Si cette garantie a été appliquée au service d'accès au site A à Z et que le bureau de Paris a connu un temps d'arrêt de 300 minutes, et celui de Lille un temps d'arrêt de 200 minutes (pour un total de 500 minutes de temps d'arrêt), le contrat de niveau de service est violé. Cependant, la formulation dans le contrat de niveau de service indique « ...chaque site client... » Une garantie doit donc être appliquée à chaque site. En appliquant les garanties de cette manière, le contrat de niveau de service ne serait pas violé, aucun des sites n'ayant subi plus de 432 minutes de temps d'arrêt. En ce qui concerne la disponibilité du service de routage, deux garanties séparées de 99 % s'appliquent :

- Disponibilité de Paris : 99 %
- Disponibilité de Lille : 99 %

Le contrat de niveau de service stipule également « ...le temps moyen de résolution des interruptions soit de 30 minutes maximum... » Outre la garantie de disponibilité de 99 %, une garantie supplémentaire qui spécifie un temps moyen d'interruption de 30 minutes maximum est inutile. Ce composant peut être ajouté aux garanties de disponibilité en tant que supplément du délai moyen de réparation. Les garanties de disponibilité doivent à présent inclure le composant de délai moyen de réparation :

- Disponibilité de Paris : 99 %, délai moyen de réparation : 30 minutes
- Disponibilité de Lille : 99 %, délai moyen de réparation : 30 minutes

En plus du composant de délai moyen de réparation, le contrat de niveau de service stipule « ...Nous garantissons moins de deux interruptions par période de 24 heures... » Cette déclaration représente la clause d'intervalle moyen entre les défaillances. La clause d'intervalle moyen entre les défaillances établit qu'il ne peut se produire plus d'une interruption par jour. Les garanties de disponibilité doivent à présent inclure le composant d'intervalle moyen entre les défaillances :

- Disponibilité de Paris : 99 %, délai moyen de réparation : 30 minutes, intervalle moyen entre les défaillances : 24 heures
- Disponibilité de Lille : 99 %, délai moyen de réparation : 30 minutes, intervalle moyen entre les défaillances : 24 heures



Une garantie semblable, mais pourtant indépendante des sites clients, doit être appliquée au service d'accès au compte client :

- Disponibilité de Paris : 99 %, délai moyen de réparation : 30 minutes, intervalle moyen entre les défaillances : 24 heures
- Disponibilité de Lille : 99 %, délai moyen de réparation : 30 minutes, intervalle moyen entre les défaillances : 24 heures
- Disponibilité de l'accès au compte client : 99 %, délai moyen de réparation : 30 minutes, intervalle moyen entre les défaillances : 24 heures

Outre la garantie de disponibilité globale de 99 %, tenez compte des autres spécifications de disponibilité suivantes :

- Une plage horaire de fonctionnement standard définie entre 7 heures et 18 heures (heure de la côte Est américaine) du lundi au vendredi, toutes les semaines.
- Pendant ces heures de fonctionnement standard, la disponibilité de l'accès aux comptes est garantie à 99,5 % sans interruption de plus de 20 minutes.

Vous pouvez créer les garanties des heures de fonctionnement en appliquant une planification pendant la création. Une planification hebdomadaire du lundi au vendredi de 7 heures à 18 heures est appliquée aux nouvelles garanties, assurant 99,5 % de disponibilité sur la période planifiée.

Les nouvelles garanties doivent être appliquées à chaque service de routage client et au service d'accès au compte client :

- Disponibilité de Paris : 99 %, délai moyen de réparation : 30 minutes, intervalle moyen entre les défaillances : 24 heures
- Disponibilité de Lille : 99 %, délai moyen de réparation : 30 minutes, intervalle moyen entre les défaillances : 24 heures
- Disponibilité de l'accès au compte client : 99 %, délai moyen de réparation : 30 minutes, intervalle moyen entre les défaillances : 24 heures
- Disponibilité de Paris : 99,5 %, du lundi au vendredi, de 7 heures à 18 heures
- Disponibilité de Lille : 99,5 %, du lundi au vendredi, de 7 heures à 18 heures
- Disponibilité de l'accès au compte client : 99,5 %, du lundi au vendredi, de 7 heures à 18 heures

Une clause supplémentaire de la garantie des heures de fonctionnement doit être prise en compte : « sans interruption de plus de 20 minutes... » Elle représente la clause de temps d'interruption maximal. Les garanties des heures de fonctionnement doivent également inclure le composant de temps d'interruption maximal :

- Disponibilité de Paris : 99 %, délai moyen de réparation : 30 minutes, intervalle moyen entre les défaillances : 24 heures
- Disponibilité de Lille : 99 %, délai moyen de réparation : 30 minutes, intervalle moyen entre les défaillances : 24 heures
- Disponibilité de l'accès au compte client : 99 %, délai moyen de réparation : 30 minutes, intervalle moyen entre les défaillances : 24 heures



- Disponibilité de Paris : 99,5 %, du lundi au vendredi, de 7 heures à 18 heures, temps d'interruption maximal : 20 minutes
- Disponibilité de Lille : 99,5 %, du lundi au vendredi, de 7 heures à 18 heures, temps d'interruption maximal : 20 minutes
- Disponibilité de l'accès au compte client : 99,5 %, du lundi au vendredi, de 7 heures à 18 heures, temps d'interruption maximal : 20 minutes

Jusqu'ici, six garanties de disponibilité différentes ont été identifiées, mais aucune d'elles ne correspond à l'élément de temps de réponse stipulé dans le contrat de niveau de service :

- Le temps de transaction moyen pour un accès initial aux comptes ne doit pas dépasser cinq secondes pour plus de 5 % de la plage horaire de fonctionnement standard, avec une exécution des transactions réussie garantie à 99 % pendant les heures de fonctionnement standard. Une transaction est réputée réussie si elle est exécutée dans un délai de 15 secondes et aucun échec de transaction ne dure plus de 20 minutes.
- La moyenne de surveillance des transactions basée sur un échantillon de cinq requêtes à émettre de manière aléatoire dans un intervalle de cinq minutes pendant les heures de fonctionnement standard, chaque requête provenant du périphérique du point d'accès client.

Les clauses du temps de réponse sont exhaustives et indiquent la manière dont le temps de réponse est mesuré. Pour prendre en charge ces composants du contrat de niveau de service, vous devez créer deux services supplémentaires en utilisant les tests du temps de réponse comme ressources surveillées.

Créez un service du temps de réponse à Paris de manière à surveiller cinq nouveaux modèles de tests du temps de réponse qui seront hébergés sur le routeur d'accès de Lille et exécutés à des intervalles de cinq minutes. Le contrat de niveau de service spécifie un seuil majeur de 5 secondes et un seuil critique de 15 secondes. Tout d'abord, vous pouvez tenir compte du fait que chaque test du temps de réponse (test SPM) doit être configuré avec un seuil majeur de 5 secondes et un seuil critique de 15 secondes. Cependant, la formulation du contrat de niveau de service suggère que cette configuration est inappropriée. Notez que la formulation « ...le temps de transaction moyen pour un accès initial aux comptes ne doit pas dépasser cinq secondes... » Vous devez surveiller le temps de réponse moyen plutôt que celui de chaque test.

Imaginez l'ensemble de résultats suivant pour le temps de réponse : 4 secondes, 3 secondes, 3 secondes, 3 secondes et 6 secondes. Le résultat de 6 secondes est supérieur au seuil de 5 secondes. Cependant, le temps de réponse moyen est inférieur à 4 secondes, ce qui ne constitue pas une violation. Pour que ce comportement soit accepté, vous ne devez pas définir de seuils sur chaque test du temps de réponse. Créez plutôt un service de temps de réponse à l'aide d'une stratégie permettant de surveiller la latence des tests du temps de réponse. La nouvelle stratégie de service doit être créée de manière à surveiller l'attribut Latest Result (dernier résultat) sur les modèles de tests du temps de réponse. Elle doit s'appliquer à un ensemble complet de règles lors de l'évaluation des temps de réponse comme suit :

- Lorsque la moyenne de toutes les ressources est supérieure à 15 000, le service est arrêté.
- Lorsque la moyenne de toutes les ressources est supérieure à 5 000, le service est détérioré.



La valeur de l'attribut Latest Result d'un modèle de test du temps de réponse représente la durée d'exécution du test le plus récent, en millisecondes. De plus, les valeurs de la stratégie de service ci-dessus sont exprimées en millisecondes. Les services du temps de réponse de Paris et de Lille doivent tous deux utiliser cette stratégie pour surveiller cinq tests du temps de réponse hébergés par le routeur d'accès du site correspondant.

Conformément aux spécifications du temps de réponse du contrat de niveau de service, deux garanties du temps de réponse des heures de fonctionnement sont nécessaires pour rechercher le temps de réponse des services créés ci-dessus :

- Temps de réponse à Paris : 95 %, du lundi au vendredi, de 7 heures à 18 heures
- Temps de réponse à Lille : 95 %, du lundi au vendredi, de 7 heures à 18 heures

Un autre composant de disponibilité est inclus dans la clause du temps de réponse :

- ...une exécution des transactions réussie garantie à 99 % pour les heures de fonctionnement standard. Une transaction est réputée réussie si elle est exécutée dans un délai de 15 secondes et qu'aucun échec de transaction ne dure plus de 20 minutes.

D'après la deuxième définition d'une garantie de disponibilité, « un service est indisponible lorsqu'il n'est pas réactif ». La spécification du contrat de niveau de service ci-dessus requiert deux autres garanties de disponibilité à 99 %, ainsi qu'un composant de temps d'interruption maximal supplémentaire.

- Temps de réponse à Paris : 95 %, du lundi au vendredi, de 7 heures à 18 heures
- Temps de réponse à Lille : 95 %, du lundi au vendredi, de 7 heures à 18 heures
- Disponibilité de Paris : 99 %, du lundi au vendredi, de 7 heures à 18 heures, temps d'interruption maximal : 20 minutes
- Disponibilité de Lille : 99 %, du lundi au vendredi, de 7 heures à 18 heures, temps d'interruption maximal : 20 minutes

Vous devez également tenir compte d'une clause relative aux opérations de maintenance dans le contrat de niveau de service :

- ...en dehors des périodes de maintenance du système planifiées entre minuit et 3 heures du matin tous les dimanches...

Pour justifier les opérations de maintenance, modifiez chaque service de manière à inclure une planification de maintenance pour cette période.



Le tableau ci-dessous répertorie tous les composants du contrat de niveau de service qui ont été pris en compte pour cette conception :

Composants de conception du contrat de niveau de service

SERVICE :	COMPOSANT DU CONTRAT DE NIVEAU DE SERVICE :
Accès au site A à Z	Contrat de niveau de service mensuel
Accès au compte client	■ Disponibilité : 99 %, délai moyen de réparation : 30 minutes, intervalle moyen entre les défaillances : 24 heures ■ Disponibilité : 99,5 %, du lundi au vendredi, de 7 heures à 18 heures, temps d'interruption maximal : 20 minutes
Routage jusqu'à Paris	■ Disponibilité : 99 %, délai moyen de réparation : 30 minutes, intervalle moyen entre les défaillances : 24 heures ■ Disponibilité : 99,5 %, du lundi au vendredi, de 7 heures à 18 heures, temps d'interruption maximal : 20 minutes
Routage jusqu'à Lille	■ Disponibilité : 99 %, délai moyen de réparation : 30 minutes, intervalle moyen entre les défaillances : 24 heures ■ Disponibilité : 99,5 %, du lundi au vendredi, de 7 heures à 18 heures, temps d'interruption maximal : 20 minutes
Temps de réponse à Paris	■ Temps de réponse : 95 %, du lundi au vendredi, de 7 heures à 18 heures ■ Disponibilité : 99 %, du lundi au vendredi, de 7 heures à 18 heures, temps d'interruption maximal : 20 minutes
Temps de réponse à Lille	■ Temps de réponse : 95 %, du lundi au vendredi, de 7 heures à 18 heures ■ Disponibilité : 99 %, du lundi au vendredi, de 7 heures à 18 heures, temps d'interruption maximal : 20 minutes



Implémentation du contrat de niveau de service pour l'accès au compte de A à Z dans SPECTRUM

Pour implémenter la conception du contrat de niveau de service décrite dans la section précédente, suivez la procédure de haut niveau ci-dessous :

1. Créez les deux services de routage et les moniteurs de ressources associés pour les routeurs et les interfaces. Vous obtenez un résultat de 6 services, regroupés en deux hiérarchies.

   - Pour chaque site, utilisez l'éditeur de services pour configurer le premier moniteur de ressources (routeur de Paris et routeur de Lille) de manière à observer l'état de contact du modèle de périphérique du routeur d'accès grâce à la stratégie de haute sensibilité de l'état de contact.
   - Pour chaque site, configurez le deuxième moniteur de ressources (interfaces de Paris et de Lille) pour observer l'état du port des interfaces de routeurs vitales à l'aide d'une stratégie d'état du port. Pensez à utiliser l'ensemble de règles Low Sensitivity (basse sensibilité) ou Percentage (pourcentage) pour la stratégie de service en fonction du nombre de modèles d'interfaces requis pour fournir l'accès.
   - Utilisez l'éditeur de services pour créer les services de routage jusqu'à Paris et Lille, qui surveillent le fonctionnement du service de leurs deux moniteurs de ressources (définis plus haut), à l'aide de la stratégie de haute sensibilité du fonctionnement du service.

2. Créez les services de temps de réponse de Paris et de Lille, ainsi que chaque modèle de test du temps de réponse (SMP) associé.

   - Utilisez l'onglet Locater de la console OneClick pour configurer 5 modèles de tests SPM pour chaque site avec les paramètres suivants :
     - Un intervalle planifié de 5 minutes (300 secondes) et les seuils désactivés
     - Une valeur de temporisation de 25 à 30 secondes
     - Définir Filter Timeout Data à FALSE pour configurer les modèles de tests de manière à ce que la valeur de temporisation soit inscrite dans l'attribut Latest Result
   - Utilisez Service Editor pour créer les moniteurs de services du temps de réponse de Paris et de Lille et garantir qu'ils surveillent les nouveaux modèles de tests du temps de réponse (SMP).
   - A l'aide de Service Policy Editor, configurez chaque service du temps de réponse de manière à ce qu'il utilise une nouvelle stratégie de service surveillant l'attribut Latest Result du test du temps de réponse, ainsi que l'intégralité de l'ensemble de règles suivant :
     - Lorsque la moyenne de toutes les ressources est supérieure à 15 000, le service est arrêté.
     - Lorsque la moyenne de toutes les ressources est supérieure à 5 000, le service est détérioré.



3. Consolidez le routage, le temps de réponse et le service d'accès client créé précédemment (dans l'exemple 2) dans des services de niveau supérieur.

   › Consolidez les services de routage et de temps de réponse des deux sites clients sous deux nouveaux services : Accès au site A à Z et Temps de réponse A à Z. Les deux nouveaux services doivent surveiller leurs composants respectifs avec une stratégie de haute sensibilité du fonctionnement du service.

   › Créez le service d'accès au compte A à Z pour surveiller les services d'accès au site A à Z, de temps de réponse A à Z et d'accès au compte client. Les nouveaux services doivent surveiller leurs composants avec une stratégie de haute sensibilité du fonctionnement du service.

4. Configurez les règles du contrat de niveau de service.

   › Après avoir apporté les modifications à la hiérarchie de services, naviguez jusqu'à l'onglet SLA dans Service Editor. Créez un contrat de niveau de service par rapport au service d'accès au compte A à Z en choisissant une période de contrat mensuelle. Ne créez pas maintenant les garanties du service d'accès au compte A à Z.

   › Lancez l'éditeur Guarantee Editor, en sélectionnant le nouveau contrat de niveau de service.

   › Utilisez l'éditeur Guarantee Editor pour créer chacune des dix garanties (8 garanties de disponibilité et 2 garanties de temps de réponse) identifiées dans la section précédente.

   › Appliquez les spécifications de délai moyen de réparation, d'intervalle moyen entre les défaillances et de temps d'interruption maximal aux garanties appropriées.

   Remarque : La fonctionnalité permettant d'associer les heures de fonctionnement à ces garanties est prévue dans SPECTRUM 8.1. Ignorez la restriction relative aux heures de fonctionnement dans les versions antérieures à 8.1.

Une garantie du contrat de niveau de service est violée dans les cas suivants :

- Le seuil d'une garantie est dépassé.
- Le seuil d'une garantie supplémentaire est dépassé (à savoir, le temps d'interruption maximal, le délai moyen de réparation ou l'intervalle moyen entre les défaillances).

Lorsque le seuil du temps d'interruption maximal est franchi, la garantie supplémentaire enfreint immédiatement le contrat de niveau de service. Si le seuil du délai moyen de réparation ou de l'intervalle moyen entre les défaillances est dépassé, la garantie fait passer le contrat de niveau de service à l'état « à risque » puisqu'il est impossible de déterminer si ce seuil a été franchi avant le terme du contrat.

L'état du contrat de niveau de service équivaut à celui de sa garantie la plus basse. Le non respect d'une garantie entraîne la violation du contrat de niveau de service pour la période correspondante. Lorsque la période du contrat de niveau de service se renouvelle, le contrat repasse à l'état « non affecté ».



Une garantie du contrat de niveau de service est violée dans les cas suivants :

- Le seuil d'une garantie est dépassé.
- Le seuil d'une garantie supplémentaire est dépassé (à savoir, le temps d'interruption maximal, le délai moyen de réparation ou l'intervalle moyen entre les défaillances).

Lorsque le seuil du temps d'interruption maximal est franchi, la garantie supplémentaire enfreint immédiatement le contrat de niveau de service. Si le seuil du délai moyen de réparation ou de l'intervalle moyen entre les défaillances est dépassé, la garantie fait passer le contrat de niveau de service à l'état « à risque » puisqu'il est impossible de déterminer si ce seuil a été franchi avant le terme du contrat.

L'état du contrat de niveau de service équivaut à l'état de sa garantie la plus basse. Le non respect d'une garantie entraîne la violation du contrat de niveau de service pour la période correspondante. Lorsque la période du contrat de niveau de service se renouvelle, le contrat repasse à l'état « non affecté ».

Génération de rapports sur les services et les contrats de niveau de service

Les rapports de disponibilité des services et des contrats de niveau de service sont des composants principaux de la solution Service Management. Ces rapports constituent un complément du service et du processus de modélisation des contrats de niveau de service et offrent un aperçu des performances des composants de service sur plusieurs périodes. Les rapports de disponibilité des services et des contrats de niveau de service peuvent être classés en deux groupes : rapports clients et rapports internes.

Les rapports clients offrent des informations relatives à l'état de disponibilité des services et des contrats de niveau de service. Ils peuvent être fournis aux clients des services. Les contrats de niveau de service stipulent souvent que les client recevront les rapports de services et de contrats de niveau de service pour chaque période du contrat. Les rapports clients récapitulent souvent l'état. Par exemple, un rapport client de disponibilité n'indique que deux mesures : le temps de disponibilité et le temps d'arrêt. De même, un rapport client de contrat de niveau de service n'indique que deux mesures : le respect ou la violation.

Les rapports internes sont conçus pour fournir un vaste ensemble de données détaillées à l'usage du fournisseur de services ou de l'entreprise. Contrairement au contrat client de disponibilité des services, un rapport interne de disponibilité des services affiche les heures de maintenance, la perte de temps de gestion, etc. De même, un rapport interne de contrat de niveau de service comprend tous les états possibles du contrat (absence d'affectation, avertissement concernant le respect ou la violation, etc.).

D'autres rapports internes peuvent récapituler les services en faisant apparaître le temps d'arrêt le plus important ou les ressources de services responsables de la plupart des temps d'arrêt. Les rapports internes ont pour but de fournir un aperçu du fonctionnement et des performances de leurs services et contrats de niveau de service sur une période donnée.



Exécution de rapports clients avec SPECTRUM Service Manager

Service Manager offre à ses utilisateurs plusieurs rapports clients différents concernant la catégorie de disponibilité des services et des contrats de niveau de service. Utilisez l'application SPECTRUM Report Manager pour générer et gérer vos rapports. Vous pouvez accéder à l'application à partir de tout ordinateur pouvant se connecter au serveur OneClick via une session Internet et sur lequel Report Manager est installé.

Pour accéder à Report Manager et exécuter des rapports :

1. Utilisez un navigateur Web pour accéder à la page Internet Report Manager à l'adresse http://*hostname*/SPECTRUM/repmgr, où *hostname* représente le nom du système OneClick et Report Manager.

2. Connectez-vous à l'application en spécifiant votre nom d'utilisateur et votre mot de passe dans la fenêtre de connexion de OneClick.

3. Dans la fenêtre Report Manager Welcome, cliquez sur le lien Begin Session.

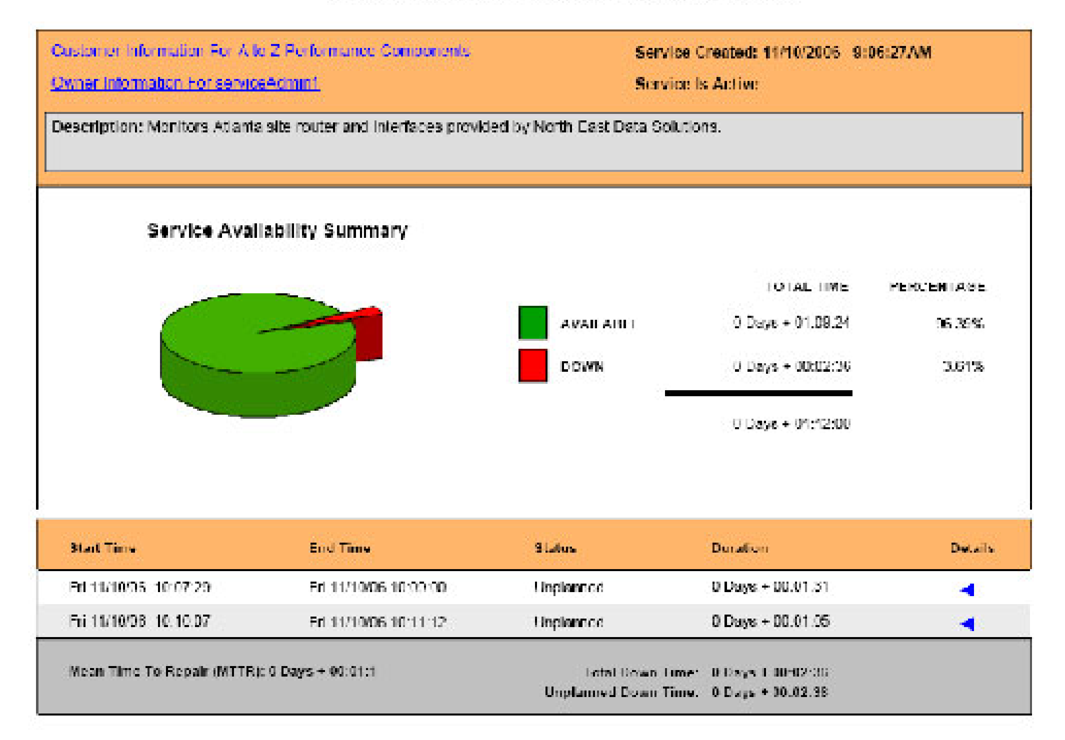
La fenêtre principale Report Manager s'affiche. Elle fournit un accès à tous les rapports et à toutes les options de gestion des rapports de votre compte. Elle répertorie tous les rapports planifiés générés ou à générer pour votre compte et tous les messages des zones de texte Message of the Day et What's New envoyés par un administrateur de Report Manager. Pour obtenir une description complète de Report Manager et de son utilisation, reportez-vous au manuel *Report Manager User Guide*.

Les sections suivantes décrivent les rapports clients.



Service Availability by : Name, Customer, Owner (Disponibilité du service par nom, client et propriétaire)

Ce rapport contient un graphique circulaire indiquant le temps d'activité/d'arrêt et le pourcentage de disponibilité pour la période concernée. Un tableau répertoriant tous les arrêts indique l'heure de début, l'heure de fin, la durée et les remarques concernant les interruptions. De plus, un sous-rapport contenant des informations détaillées sur chaque interruption du tableau est également disponible. Vous pouvez générer plusieurs rapports de disponibilité des services par nom, client ou propriétaire du service.

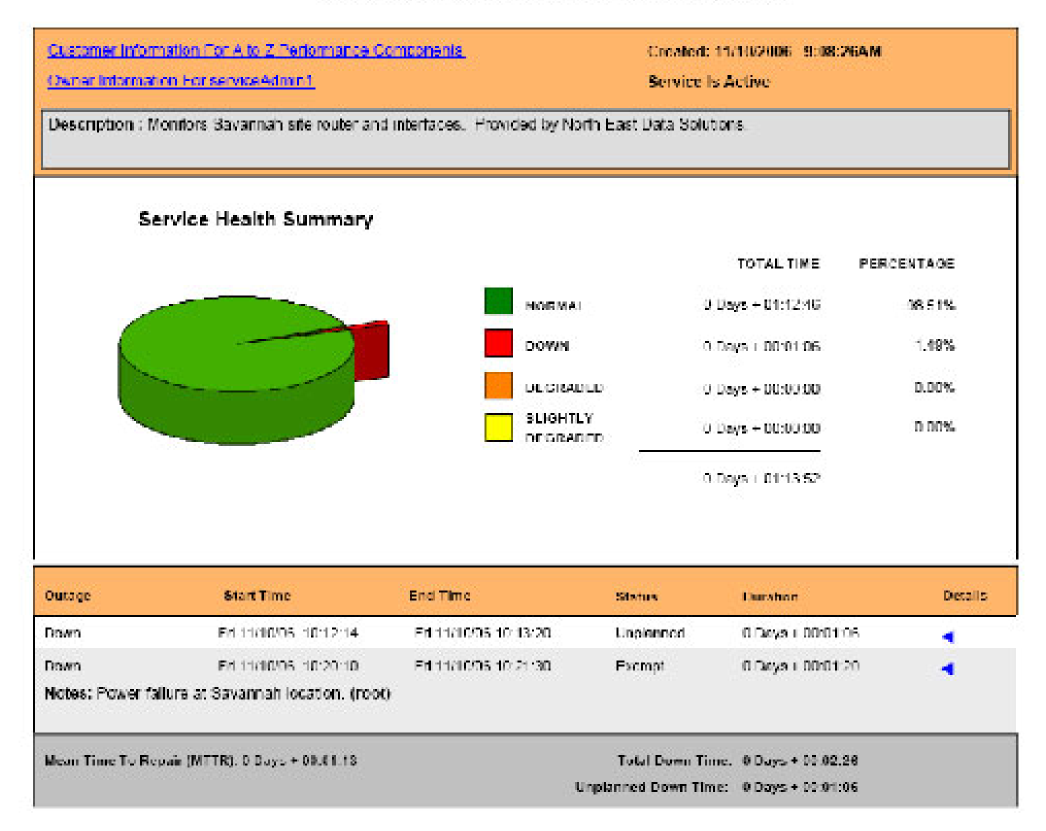




Service Availability Variable Health Level (Niveau de fonctionnement variable selon la disponibilité du service)

Ce rapport est semblable au rapport de disponibilité des services, mais il vous permet d'inclure l'heure à laquelle un service a été détérioré ou légèrement détérioré, le cas échéant. Un graphique circulaire comprenant tous les états de fonctionnement du service est affiché, de même qu'un calcul du pourcentage de disponibilité pour la période concernée. Toutes les interruptions incluses sont répertoriées dans le sous-rapport indiquant les informations détaillées correspondantes.







Service Summary by : Name, Customer, Owner (Récapitulatif des services par nom, client et propriétaire)

Ce rapport répertorie plusieurs services en fonction de leur nom, de leur client ou de leur propriétaire, ainsi que les temps d'interruption et le pourcentage de disponibilité.

SPECTRUM **Summary of Service Availability**

Date Range: 11/10/2006 12:00:00AM to 11/10/2006 10:36:53AM

Service Name	Up	Down	Degraded	Slightly Degraded
A to Z Account Access				
Percentage	70.10%	13.62%	0.00%	7.28%
Total Time	0 Dy + 00:42:12	0 Dy + 00:07:16	0 Dy + 00:00:00	0 Dy + 00:03:53
Outage Count/ MTTR		6 / 0 Dy + 00:01:27	0 / 0 Dy + 00:00:00	2 / 0 Dy + 00:03:53
A to Z Site Access				
Percentage	92.63%	7.37%	0.00%	0.00%
Total Time	0 Dy + 01:03:17	0 Dy + 00:05:02	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/ MTTR		4 / 0 Dy + 00:01:16	0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00
Atlanta Routing				
Percentage	96.77%	3.23%	0.00%	0.00%
Total Time	0 Dy + 01:17:50	0 Dy + 00:02:36	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/ MTTR		2 / 0 Dy + 00:01:18	0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00
Customer Account Access Service				
Percentage	[illegible]	5.17%	0.00%	12.27%
Total Time	0 Dy + 00:39:24	0 Dy + 00:02:25	0 Dy + 00:00:00	0 Dy + 00:05:51
Outage Count/ MTTR		2 / 0 Dy + 00:01:12	0 / 0 Dy + 00:00:00	3 / 0 Dy + 00:05:51
Web Service				
Percentage	86.56%	4.14%	0.00%	9.30%
Total Time	0 Dy + 00:43:36	0 Dy + 00:02:06	0 Dy + 00:00:00	0 Dy + 00:04:41
Outage Count/ MTTR		1 / 0 Dy + 00:02:06	0 / 0 Dy + 00:00:00	2 / 0 Dy + 00:04:41
Savannah Routing				
Percentage	98.60%	1.40%	0.00%	0.00%
Total Time	0 Dy + 01:17:21	0 Dy + 00:01:06	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/ MTTR		1 / 0 Dy + 00:01:06	0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00
Database Service				
Percentage	96.96%	0.50%	0.00%	2.37%
Total Time	0 Dy + 00:47:18	0 Dy + 00:00:20	0 Dy + 00:00:00	0 Dy + 00:01:10
Outage Count/ MTTR		1 / 0 Dy + 00:00:20	0 / 0 Dy + 00:00:00	1 / 0 Dy + 00:01:10
Atlanta Resp Time				
Percentage	100.00%	0.00%	0.00%	0.00%
Total Time	0 Dy + 00:56:30	0 Dy + 00:00:00	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/ MTTR		0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00
Savannah Response Time				
Percentage	100.00%	0.00%	0.00%	0.00%
Total Time	0 Dy + 00:56:09	0 Dy + 00:00:00	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/ MTTR		0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00

Service Summary Variable Health Level (Niveau de fonctionnement variable selon le récapitulatif des services)

Ce rapport dresse un tableau des services. Les colonnes présentent un récapitulatif des données à chaque niveau de fonctionnement des services que vous avez choisi d'inclure au rapport, comme pour le rapport précédent. Vous pouvez choisir d'afficher l'état arrêté uniquement, l'état arrêté et détérioré ou l'état arrêté, détérioré et légèrement détérioré. Un sous-rapport comportant des informations plus détaillées sur les interruptions est disponible pour chaque service répertorié dans le tableau.



SLA Detail By Customer (Détails du contrat de niveau de service par client)

Vous pouvez générer ce rapport pour une ou plusieurs périodes du contrat de niveau de service. Le rapport comprend un graphique circulaire qui affiche le pourcentage de garanties pour chaque période signalée respectée ou violée. Chaque garantie, de même que l'état de chaque période, est indiqué sous le graphique. Pour chaque période, vous pouvez ouvrir un sous-rapport incluant des informations détaillées sur les interruptions de la garantie spécifique, y compris les exemptions relatives aux interruptions. Si vous exécutez le rapport en fonction du client, un rapport séparé est généré pour chaque contrat de niveau de service associé. Vous pouvez fournir le rapport au client à la fin de chaque période.

SPECTRUM

Service Level Agreement Detail Report

Date Range: 11/10/2006 12:50:03AM to 11/10/2006 3:20:12PM

A to Z Customer Account Access SLA

Guarantees Customer Account Access Service Service

Customer Information For A to Z Performance Components

Description: SLA for A to Z Performance Components provided by North East Data Solutions

Guarantee Status Distribution

Compliant

Violated

Customer Access Availability - Monitors Customer Account Access Service Service			Availability Report
Compliant	Nov 10, 2006 - Nov 11, 2006	Availability	Period Details
Cust Access Business Hours Availability - Monitors Customer Account Access Service Service			Availability Report
Compliant	Nov 10, 2006 - Nov 11, 2006	Availability	Period Details
Atlanta Routing 7x24 Availability - Monitors Atlanta Routing Service			Availability Report
Compliant	Nov 10, 2006 - Nov 11, 2006	Availability	Period Details
Atlanta Routing Business Hours Availability - Monitors Atlanta Routing Service			Availability Report
Compliant	Nov 10, 2006 - Nov 11, 2006	Availability	Period Details
Savannah Routing 7x24 Availability - Monitors Savannah Routing Service			Availability Report
Compliant	Nov 10, 2006 - Nov 11, 2006	Availability	Period Details
Savannah Routing Business Hours Availability - Monitors Savannah Routing Service			Availability Report
Compliant	Nov 10, 2006 - Nov 11, 2006	Availability	Period Details

Report Generated 11/10/2006 3:20:12PM SPECTRUM SERVICE MANAGER Page 1 of 2



SLA Inventory by Customer (Inventaire du contrat de niveau de service par client)

Ce rapport indique la configuration de chaque contrat de niveau de service et chaque garantie d'un client spécifique. Il est utile de générer ce rapport pour un client lorsque les modèles de contrats de niveau de service et de garanties sont créés pour la première fois. L'utilisateur doit pouvoir comparer la configuration avec le document du contrat de niveau de service pour vérifier que toutes les garanties ou tous les objectifs de niveau de service sont atteints.

SPECTRUM

SLA Inventory Report
for A to Z Performance Components

Report Generated: 11/10/2006 10:20:43AM

A to Z Customer Account Access SLA	Availability Threshold	Response Time Threshold	MAX Outage Time	Mean Time To Repair	Mean Time Between Faults
Customer Access Availability	0 Days + 00:14:24		0 Days + 00:00:00	0 Days + 00:30:00	1 Day + 00:00:00
Cust Access Business Hours Availability	0 Days + 00:07:12		0 Days + 00:20:00	0 Days + 00:00:00	0 Days + 00:00:00
Atlanta Routing 7x24 Availability	0 Days + 00:14:24		0 Days + 00:00:00	0 Days + 00:30:00	1 Day + 00:00:00
Atlanta Routing Business Hours Availability	0 Days + 00:07:12		0 Days + 00:20:00	0 Days + 00:00:00	0 Days + 00:00:00
Savannah Router 7x24 Availability	0 Days + 00:14:24		0 Days + 00:00:00	0 Days + 00:30:00	1 Day + 00:00:00
Savannah Routing Business Hours Availbility	0 Days + 00:07:12		0 Days + 00:20:00	0 Days + 00:00:00	0 Days + 00:00:00
Atlanta Resp Time Time Business Hours Availability	0 Days + 00:14:24		0 Days + 00:20:00	0 Days + 00:00:00	0 Days + 00:00:00
Savannah Resp Time Business Hours Availability	0 Days + 00:14:24		0 Days + 00:20:00	0 Days + 00:00:00	0 Days + 00:00:00
Atlanta Business Hours Response Time		0 Days + 01:12:00			
Savannah Business Hours Response Time		0 Days + 01:12:00			

Rapports internes de SPECTRUM Service Manager

Service Manager offre à ses utilisateurs plusieurs rapports internes différents concernant la catégorie de disponibilité des services et des contrats de niveau de service. Les sections suivantes décrivent les rapports internes.



Service Health by Service Name (Fonctionnement du service par nom de service)

Ce rapport ressemble beaucoup à un rapport de disponibilité des services, mais il comprend tous les niveaux de fonctionnement des services, y compris la maintenance et la perte de gestion. Il peut être exécuté pour les services, tout comme pour les moniteurs de ressources. Il comprend un graphique circulaire indiquant le pourcentage de valeur de fonctionnement de chaque service. Ce rapport contient également un tableau indiquant l'interruption de tous les types de fonctionnement de service, y compris des remarques concernant les interruptions et des liens vers des informations détaillées. Le rapport de fonctionnement de service fournit aux utilisateurs de gestionnaires de services des informations très précises sur les performances d'un service sur une période donnée.

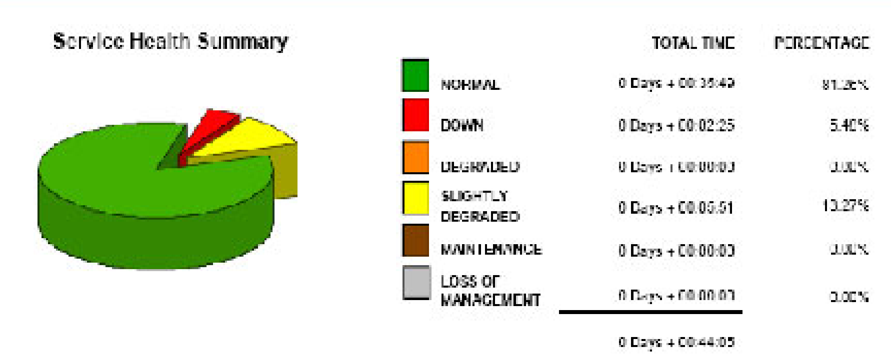
SPECTRUM

Service Health Report
for Service CUSTOMER ACCOUNT ACCESS SERIVCE

Date Range: 11/10/2006 12:00:00AM to 11/10/2006 10:23:15AM

Created: 11/10/2006 9:38:13AM
Service Is Active

Description : Monitors the overall availability of the Customer Account Access Service provided by North East Data Solutions.



Outage	Start Time	End Time	Status	Duration	Details
Down	Fri 11/10/06 10:05:35	Fri 11/10/06 10:07:40	Unplanned	0 Days + 00:02:05	◄
Down	Fri 11/10/06 10:13:26	Fri 11/10/06 10:13:46	Unplanned	0 Days + 00:00:20	◄
Mean Time To Repair (MTTR): 0 Days + 00:01:12			Total Down Time:	0 Days + 00:02:25	
			Unplanned Down Time	0 Days + 00:02:25	

Outage	Start Time	End Time	Status	Duration	Details
Slightly Degraded	Fri 11/10/06 10:02:52	Fri 11/10/06 10:05:35	Unplanned	0 Days + 00:02:43	◄
Slightly Degraded	Fri 11/10/06 10:07:40	Fri 11/10/06 10:09:38	Unplanned	0 Days + 00:01:58	◄
Slightly Degraded	Fri 11/10/06 10:13:46	Fri 11/10/06 10:14:56	Unplanned	0 Days + 00:01:10	◄
Mean Time To Repair (MTTR): 0 Days + 00:01:57			Total Slightly Degraded Time:	0 Days + 00:05:51	
			Unplanned Slightly Degraded Time	0 Days + 00:05:51	



Service Inventory (Inventaire des services)

Ce rapport illustre la structure de tous les services, moniteurs de ressources et ressources modélisées dans le système. Il peut servir à capturer un « instantané » de la configuration d'inventaire des services pendant la période en cours.

SPECTRUM

Service and Resource Monitor Inventory

Report Generated: 11/10/2006 10:38:02AM

Service Or Resource Monitor			Resources	Resource Class
(S)	A to Z Account Access	(S)	A to Z Site Access	Service Mgt Component
		(S)	A to Z Site Resp Time	Service Mgt Component
		(S)	Customer Account Access Serivce	Service Mgt Component
(S)	A to Z Site Access	(S)	Atlanta Routing	Service Mgt Component
		(S)	Savannah Routing	Service Mgt Component
(S)	A to Z Site Resp Time	(S)	Atlanta Resp Time	Service Mgt Component
		(S)	Savannah Response Time	Service Mgt Component
(S)	Atlanta Resp Time		Atlanta Resp 1	Response Time Test
			Atlanta Resp 2	Response Time Test
			Atlanta Resp 3	Response Time Test
			Atlanta Resp 4	Response Time Test
			Atlanta Resp 5	Response Time Test
(S)	Atlanta Routing	(RM)	Router Contact	Service Mgt Component
		(RM)	Port Status	Service Mgt Component
(S)	Customer Account Access Service	(S)	Web Service	Service Mgt Component
		(S)	Database Service	Service Mgt Component
(S)	Database Service	(RM)	Devices	Service Mgt Component
		(RM)	Processes	Service Mgt Component
(RM)	Device		wiljo18-sol	Workstation-Server
			HDMSYRKAPPS2	Workstation-Server
(RM)	Devices		RK4DCA20	Workstation-Server
			NT3 FASC HVNY	Workstation-Server
(RM)	Port Status		Cat65R6500_179_Fi0/1	Port
			Cat65R6500_179_Fi0/2	Port

S - Indicates Service
RM - Indicates Resource Monitor

Report Generated 11/10/2006 10:38:02AM SPECTRUM SERVICE MANAGER Page 1 of 2



Top N Worst Performing Services (Les N services les moins performants)

Ce rapport vous permet de visualiser les N services les moins performants pour une période donnée. Un graphique à barres présente un récapitulatif de chaque service. Un tableau présentant un récapitulatif des informations de disponibilité de chaque service est également disponible. Ce tableau contient des liens vers un rapport de disponibilité des services plus détaillé. Ce rapport est utile aux utilisateurs chargés de la gestion de services car il leur permet d'obtenir des informations concernant les services les moins performants sur n'importe quelle période donnée.

SPECTRUM **Worst Performing Services By Total Outage Time**

Outage Time For Services

In Minutes

Service Name	Up	Down	Degraded	Slightly Degraded
A to Z Account Access				
Percentage	76.37%	14.33%	0.00%	9.30%
Total Time	0 Dy + 00:31:37	0 Dy + 00:05:56	0 Dy + 00:00:00	0 Dy + 00:03:51
Outage Count/ MTTR		4 / 0 Dy + 00:01:29	0 / 0 Dy + 00:00:00	2 / 0 Dy + 00:03:51
A to Z Site Access				
Percentage	93.44%	6.56%	0.00%	0.00%
Total Time	0 Dy + 00:52:10	0 Dy + 00:03:42	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/ MTTR		3 / 0 Dy + 00:01:14	0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00
Atlanta Routing				
Percentage	96.20%	3.80%	0.00%	0.00%
Total Time	0 Dy + 01:05:53	0 Dy + 00:02:38	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/ MTTR		2 / 0 Dy + 00:01:18	0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00

Report Generated 11/10/2006 at 10:14:56AM SPECTRUM SERVICE MANAGER Page 1 of 2



Top N Worst Performing Services Including All Outage Types (Les N services les moins performants incluant tous les types d'interruptions)

Ce rapport est semblable au rapport Top N Worst Performing Service, mais il comprend l'heure à laquelle le service est détérioré ou légèrement détérioré en plus du temps d'arrêt. Un récapitulatif des informations de disponibilité et des liens vers les rapports de disponibilité des services plus détaillés sont disponibles pour chaque modèle de service. Le rapport fournit des informations très détaillées pour l'utilisateur du gestionnaire de services, notamment les services qui ont subi l'interruption la plus longue sur une période spécifique.

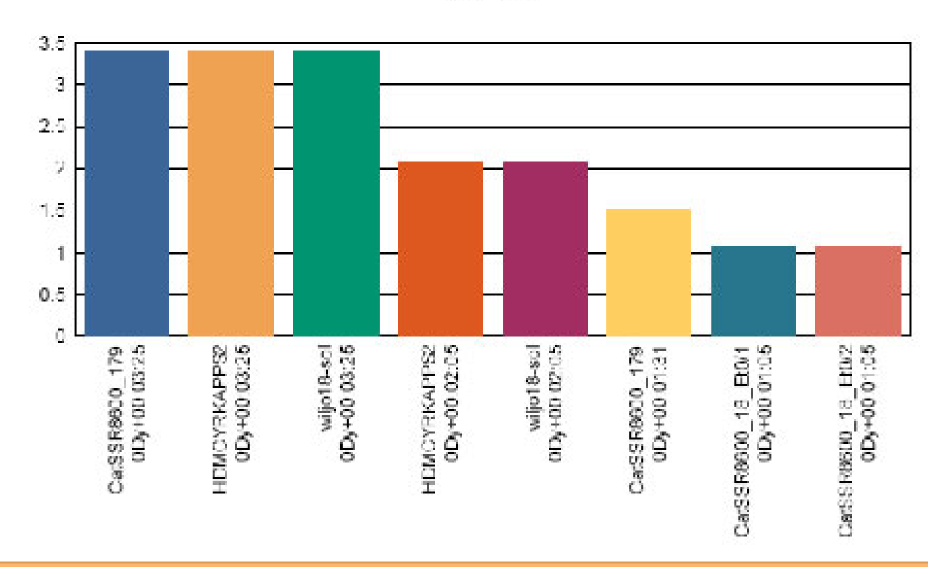
Top N Worst Service Outages (Les N pires interruptions de service)

Ce rapport vous permet de visualiser les N pires interruptions de service qui ont provoqué un temps d'arrêt des services. C'est un outil utile permettant de présenter un récapitulatif des pires interruptions de service d'une période donnée. Il peut également mettre en évidence des zones au sein de la hiérarchie de services qui manquent de redondance pour éviter les temps d'arrêt du service.



SPECTRUM **Worst Service Outages By Resource**

Selected Date Range: 11/10/2006 12:00:00AM to 11/10/2006 10:17:09AM



Resource	Outage Duration	Impacted Service	Impacted Customers
wiljo18-sol	0 Days + 00:03:25	A to Z Account Access	Customer Information
HDMCYRKAPPS2	0 Days + 00:03:25	A to Z Account Access	Customer Information
CatSSR8600_179	0 Days + 00:03:25	A to Z Account Access	Customer Information
wiljo18-sol	0 Days + 00:02:05	Web Service	
wiljo18-sol	0 Days + 00:02:05	Customer Account Access Service	
HDMCYRKAPPS2	0 Days + 00:02:05	Customer Account Access Service	
CatSSR8600_179	0 Days + 00:01:31	Atlanta Routing	Customer Information
CatSSR8600_179	0 Days + 00:01:31	A to Z Site Access	
CatSSR8600_18_Bd/1	0 Days + 00:01:05	A to Z Account Access	Customer Information
CatSSR8600_18_Bd/2	0 Days + 00:01:05	A to Z Account Access	Customer Information

Report Generated 11/10/2006 at 10:17:10AM SPECTRUM SERVICE MANAGER Page 1

Top N Worst Service Resources by Total Downtime (Les N pires ressources du service par temps d'arrêt total)

Ce rapport présente un récapitulatif des informations concernant le temps d'arrêt total du service provoqué par chaque ressource. Il met en évidence l'effet cumulatif de chaque interruption de ressource qui provoque un temps d'arrêt d'un ou de plusieurs services. Ce rapport peut notamment servir à identifier les ressources de services représentant des sources chroniques de problèmes au sein d'une hiérarchie de modélisation des services.



SPECTRUM

Worst Service Resources by Total Service Down Time

Selected Date Range: 11/10/2006 12:00:00AM to 11/10/2006 4:00:10PM

Resource Name	Service Outages	Average Service Outage	Total Service Outage Time	Resource Owner
RK4DCA20	0	0 Days + 01:31:40	0 Days + 09:10:00	0
NT3-RASC-HVNY	6	0 Days + 01:31:40	0 Days + 09:10:00	Resco Helpdesk 212-362-2000
wiljo10-sol	3	0 Days + 00:02:31	0 Days + 00:07:35	SNMP Research Inc., +1 (865) 57
HOMCY-RA-1P22	3	0 Days + 00:02:31	0 Days + 00:07:35	0
CatSSR8600_179	3	0 Days + 00:02:09	0 Days + 00:06:27	Concord CA Hardware Lab Admi
CatSSR8600_18	3	0 Days + 00:01:11	0 Days + 00:03:33	Concord CA Hardware Lab Admi
CatSSR8600_18_Et0/1	1	0 Days + 00:01:05	0 Days + 00:01:05	Concord CA Hardware Lab Admi
CatSSR8600_18_Et0/2	1	0 Days + 00:01:05	0 Days + 00:01:05	Concord CA Hardware Lab Admi
CatSSR8600_18_Et0/3	1	0 Days + 00:01:06	0 Days + 00:01:06	Concord CA Hardware Lab Admi

SLA Status Current and Recent by Customer (Etats actuels et récents du contrat de niveau de service par client)

Ce rapport représente un moyen rapide d'obtenir un récapitulatif de l'état du contrat de niveau de service pour des périodes en cours ou récentes. Il inclut les états de contrats de niveau de service non affectés, respectés, d'avertissement et violés, ainsi que des sous-rapports détaillés indiquant les résultats de garanties spécifiques. Ce rapport peut être exécuté pour des contrats de niveau de service sélectionnés ou ceux d'un client spécifique. Il peut permettre une étude rapide de l'état de nombreux contrats de niveau de service pour tous les clients.

SPECTRUM

SLA Status
Current and Most Recent Periods

Report Generated: 11/10/2006 4:12:34PM

Service Level Agreement	Period	Status	Customer
A to Z Customer Account Access SLA	Nov 10 - Nov 11, 2006	Warned	A to Z Performance Components
A to Z Billing Service SLA	Nov 1 - Dec 1, 2006	Unaffected	A to Z Performance Components
BW Tech Provisioning SLA	Nov 1 - Dec 1, 2006	Unaffected	BW TECH
BW Tech Customer Account Access S	Nov 1 - Dec 1, 2006	Unaffected	BW TECH



SLA Summary by : Name, Customer, Status (Récapitulatif des contrats de niveau de service par nom, client et état)

Ce rapport produit un tableau récapitulatif des états de contrats de niveau de service pendant une ou plusieurs périodes. Il peut être généré par nom de contrat de niveau de service, par nom de client ou simplement organisé par état. Le rapport fournit une référence résumée pour plusieurs contrats de niveau de service ou plusieurs périodes. Vous avez accès à des sous-rapports détaillés indiquant les résultats de garanties spécifiques.



Service Level Agreement
Summary By Customer

Date Range 11/10/2006 12:00:00AM to 11/10/2006 4:14:19PM

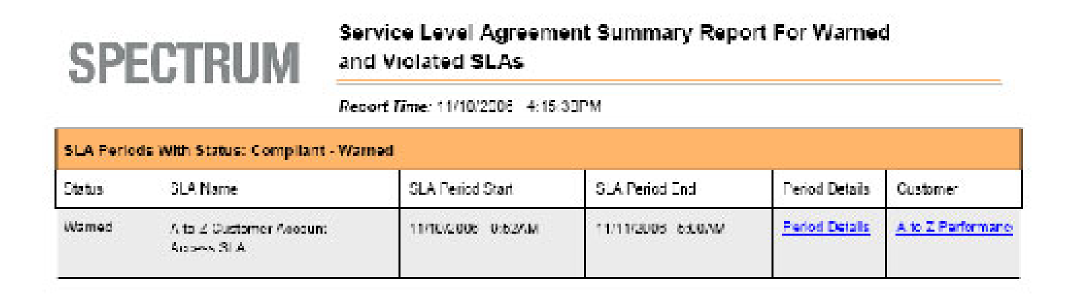
A to Z Performance Components				
Status	**SLA Name**	**SLA Period Start**	**SLA Period End**	**Period Details**
Compliant	A to Z Customer Account Access SLA	11/10/2006 9:52:21AM	11/11/2006 6:00:00AM	Period Details
Compliant	A to Z Billing Service SLA	11/1/2006 6:00:00AM	12/1/2006 6:00:00AM	Period Details

BW TECH				
Status	**SLA Name**	**SLA Period Start**	**SLA Period End**	**Period Details**
Compliant	BW Tech Provisioning SLA	11/1/2006 5:00:00AM	12/1/2006 5:00:00AM	Period Details
Compliant	BW Tech Customer Account Access SLA	11/1/2006 5:00:00AM	12/1/2006 5:00:00AM	Period Details



SLA Summary Warned or Violated (Récapitulatif des avertissements et violations dans les contrats de niveau de service)

Ce rapport produit un tableau des contrats de niveau de service actuellement à l'état d'avertissement ou de violation. Le tableau fournit également l'accès à un sous-rapport indiquant des informations détaillées sur une interruption de garantie pendant la période en cours. C'est un outil très utile pour l'utilisateur du gestionnaire de services, car il lui permet de visualiser les contrats de niveau de service qui ne fonctionnent pas correctement pendant la période en cours.



SPECTRUM

Service Level Agreement Summary Report For Warned and Violated SLAs

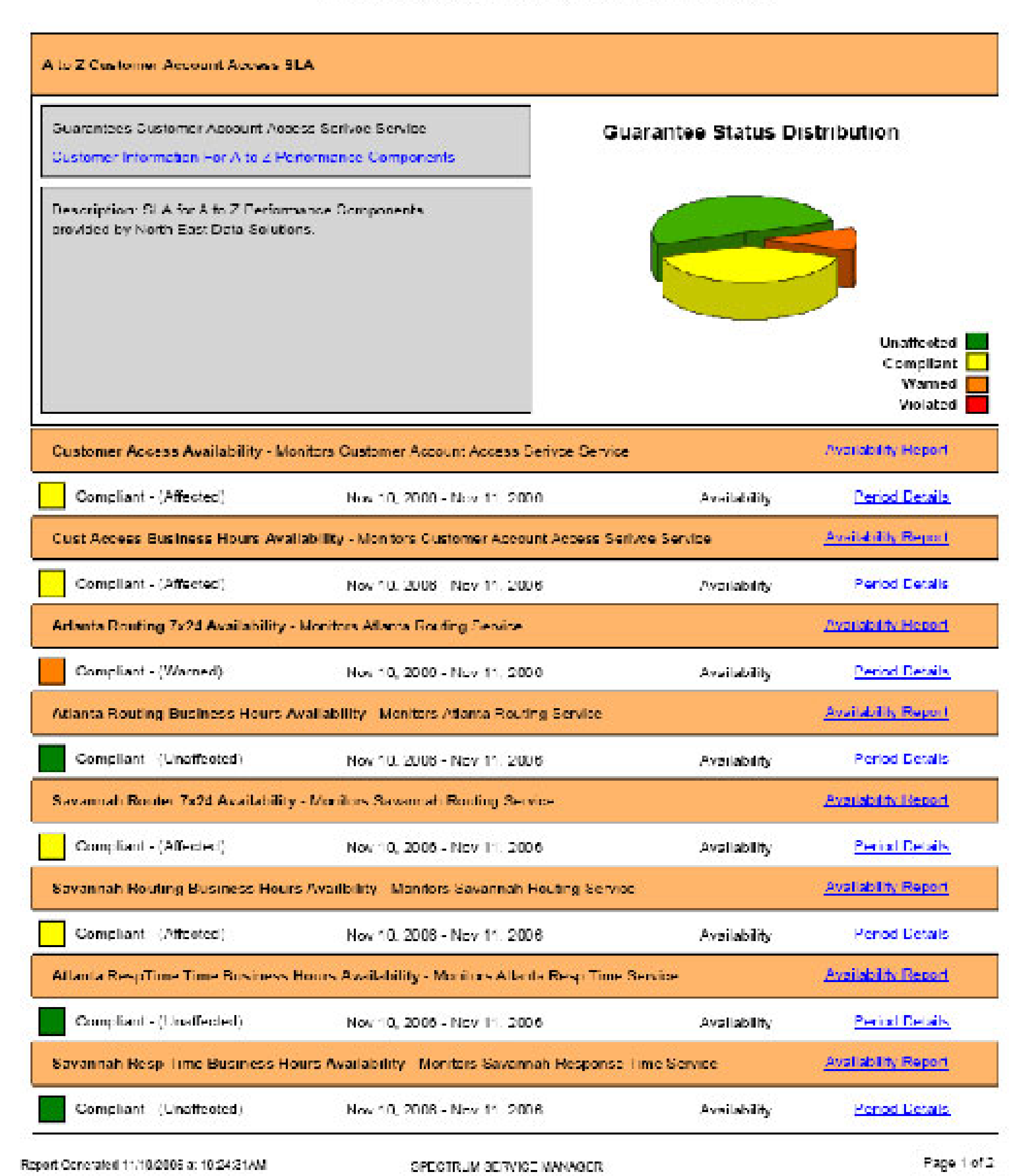
Report Time: 11/10/2006 4:15:30PM

SLA Periods With Status: Compliant - Warned					
Status	SLA Name	SLA Period Start	SLA Period End	Period Details	Customer
Warned	A to Z Customer Account: Access SLA	11/10/2006 [illegible]	11/11/2006 [illegible]	Period Details	A to Z Performanc

SLA Detail By : SLA Name, Time Range, Last N Periods (Détails du contrat de niveau de service par nom, plage horaire et N dernières périodes)

Ce rapport est similaire au rapport SLA Detail By SLA Customer, mis à part le fait qu'il affiche toutes les valeurs d'état de contrats de niveau de service, y compris l'état non affecté, respecté, d'avertissement et violé. Les informations détaillées sont fournies dans un sous-rapport comprenant les interruptions de garantie d'une période spécifique. Ceci est utile pour obtenir des informations détaillées sur chaque contrat de niveau de service d'une ou plusieurs périodes.




SPECTRUM

Service Level Agreement Detail Report

Date Range: 11/10/2006 12:00:00AM to 11/10/2006 10:24:30AM

A to Z Customer Account Access SLA

Guarantees Customer Account Access Serivce Service
Customer Information For A to Z Performance Components

Description: SLA for A to Z Performance Components provided by North East Data Solutions.

Customer Access Availability - Monitors Customer Account Access Serivce Service			Availability Report
Compliant - (Affected)	Nov 10, 2006 - Nov 11, 2006	Availability	Period Details
Cust Access Business Hours Availability - Monitors Customer Account Access Serivce Service			Availability Report
Compliant - (Affected)	Nov 10, 2006 - Nov 11, 2006	Availability	Period Details
Atlanta Routing 7x24 Availability - Monitors Atlanta Routing Service			Availability Report
Compliant - (Warned)	Nov 10, 2006 - Nov 11, 2006	Availability	Period Details
Atlanta Routing Business Hours Availability - Monitors Atlanta Routing Service			Availability Report
Compliant - (Unaffected)	Nov 10, 2006 - Nov 11, 2006	Availability	Period Details
Savannah Router 7x24 Availability - Monitors Savannah Routing Service			Availability Report
Compliant - (Affected)	Nov 10, 2006 - Nov 11, 2006	Availability	Period Details
Savannah Routing Business Hours Availbility - Monitors Savannah Routing Service			Availability Report
Compliant - (Affected)	Nov 10, 2006 - Nov 11, 2006	Availability	Period Details
Atlanta RespTime Time Business Hours Availability - Monitors Atlanta Resp Time Service			Availability Report
Compliant - (Unaffected)	Nov 10, 2006 - Nov 11, 2006	Availability	Period Details
Savannah Resp Time Business Hours Availability - Monitors Savannah Response Time Service			Availability Report
Compliant - (Unaffected)	Nov 10, 2006 - Nov 11, 2006	Availability	Period Details

Report Generated 11/10/2006 at 10:24:31AM SPECTRUM SERVICE MANAGER Page 1 of 2



SOUS-RAPPORTS DÉTAILLÉS DE PÉRIODES

Guarantee Detail Report

SPECTRUM

Period Start: 11/10/2006 5:00:00AM
Period End: 11/11/2006 5:00:00AM
Activation Time: 11/10/2006 9:52:21AM

Atlanta Routing 7x24 Availability

Compliant - (Warned)

Guarantee Configuration

Guarantees 99.90 Availability

Warning Threshold: 0 Days + 00:11:31 or 80.00% of violation threshold

Violation Threshold: 0 Days + 00:14:24

Period Performance

Statistic	Status	Threshold	Value
DOWN TIME	Compliant	0 Days + 00:14:24	0 Days + 00:02:36
MOT	Disabled	0 Days + 00:00:00	0 Days + 00:01:31
MTTR	Compliant	0 Days + 00:30:00	0 Days + 00:01:18
MTBF	At Risk	1 Day + 00:00:00	0 Days + 00:01:37

Summary of Outages

Unplanned
Planned
Exempt

Related Incidents

Start Time	End Time	Outage Duration	Outage Time This Period	Incident Status
Fri 11/10/06 10:07:29	Fri 11/10/06 10:09:00	0 Days +00:01:31	0 Days + 00:01:31	Unplanned
Fri 11/10/06 10:11:07	Fri 11/10/06 10:11:12	0 Days +00:01:05	0 Days + 00:01:05	Unplanned
			0 Days + 00:02:36	

* Indicates outage is ongoing

! Indicates time adjusted for period

Report Generated 11/10/2006 at 10:24:31AM SPECTRUM SERVICE MANAGER Page 1 of 1



Guarantee Detail Report

SPECTRUM

Period Start: 11/10/2006 5:00:00AM
Period End: 11/11/2006 5:00:00AM
Activation Time: 11/10/2006 9:52:21AM

Savannah Routing Business Hours Availability

Compliant - (Affected)

Guarantee Configuration

Guarantees 99.50 Availability

Warning Threshold: 0 Days + 00:05:45 or 80.00% of violation threshold

Violation Threshold: 0 Days + 00:07:12

Period Performance

Statistic	Status	Threshold	Value
DOWN TIME	Compliant	0 Days + 00:07:12	0 Days + 00:01:30
MOT	Compliant	0 Days + 00:20:00	0 Days + 00:01:30
MTTR	Disabled	0 Days + 00:00:00	0 Days + 00:01:30
MTBF	Disabled	0 Days + 00:00:00	0 Days + 00:00:30

Summary of Outages

Unplanned

Planned

Exempt

Related Incidents

Start Time	End Time	Outage Duration	Outage Time This Period	Incident Status
Fri 11/10/06 10:12:14	Fri 11/10/06 10:13:20	0 Days +00:01:06	0 Days + 00:01:06	Unplanned
Fri 11/10/06 10:20:10	Fri 11/10/06 10:21:30	0 Days +00:01:20	0 Days + 00:01:20	Exempt
Notes: Power failure at Savannah location. [root]				
			0 Days + 00:01:06	

* Indicates outage is ongoing

! Indicates time adjusted for period

Report Generated 11/10/2006 at 10:34:31AM SPECTRUM SERVICE MANAGER Page 1 of 1

SLA Detail with Resource Outages (Détails du contrat de niveau de service et interruptions de ressources)

Ce rapport complexe rassemble l'état des contrats de niveau de service et les interruptions de ressources associées qui ont finalement eu des conséquences sur le contrat de niveau de service pendant une période. Ce rapport est utile lorsqu'il est utilisé conjointement avec le rapport Top N Worst Resources By Total Down Time. Vous pouvez utiliser ce rapport pour indiquer les conséquences d'une ressource spécifique à un niveau très élevé. Puisqu'il fournit de nombreuses informations, il peut générer un grand nombre de pages de données sur les contrats de niveau de service, avec un nombre important d'interruption des ressources.



SPECTRUM

SLA Resource Outage Report

Date Range: November 10, 2006 to November 11, 2006

A to Z Customer Account Access SLA
Period: November 10, 2008 to November 11, 2008
Status for period: Compliant - (Warned)

Description: SLA for A to Z Performance Components provided by North East Data Solutions.

Customer Information For A to Z Performance Components

Savannah Business Hours Response Time Guarantee Compliant - (Unaffected) — Period Details

Statistic	Status	Threshold	Actual
Degraded Time	Compliant	0 Days + 01:12:00	0 Days + 00:30:00

Atlanta Business Hours Response Time Guarantee Compliant - (Unaffected) — Period Details

Statistic	Status	Threshold	Actual
Degraded Time	Compliant	0 Days + 01:12:00	0 Days + 00:30:00

Savannah Resp Time Business Hours Availability Guarantee Compliant - (Unaffected) — Period Details

Statistic	Status	Threshold	Actual
Down Time	Compliant	0 Days + 00:14:24	0 Days + 00:30:00
Maximum Outage Time	Compliant	0 Days + 00:20:00	0 Days + 00:30:00

Atlanta RespTime Time Business Hours Availability Guarantee Compliant - (UnaFfected) — Period Details

Statistic	Status	Threshold	Actual
Down Time	Compliant	0 Days + 00:14:24	0 Days + 00:30:00
Maximum Outage Time	Compliant	0 Days + 00:20:00	0 Days + 00:30:00

Savannah Routing Business Hours Availability Guarantee Compliant - (Affected) — Period Details

Statistic	Status	Threshold	Actual
Down Time	Compliant	0 Days + 00:07:12	0 Days + 00:31:06
Maximum Outage Time	Compliant	0 Days + 00:20:00	0 Days + 00:31:06

Resouce outages impacting Savannah Routing Service

Duration = 0 Days +00:01:20 From: 11/10/2008 10:20:10AM To: 11/10/2008 10:21:30AM (Exempt)

CatSSR8500_18 - Unable to contact device

Report Generated [illegible] SPECTRUM SERVICE MANAGER Page 1 of 3



Customer SLA Summary (Récapitulatif des contrats de niveau de service clients)

Ce rapport indique l'état des six dernières périodes de contrats de niveau de service pour les contrats de tous les clients. L'état comprend les quatre valeurs. Pour chaque contrat de niveau de service, un graphique récapitulatif des informations concernant les six périodes d'état est présenté dans un tableau résumant les données de chaque période, ainsi qu'un lien vers des informations d'interruption de garantie plus détaillées. Ce rapport offre aux gestionnaires de services une vue rapide des performances du contrat de niveau de service pour un client spécifique sur les six dernières périodes. Il peut également être utilisé par l'entreprise commerciale pour vérifier si le contrat de niveau de service d'un client a été respecté dans les périodes récentes.

SPECTRUM

Customer SLA Summary Report
A to Z Performance Components

Report Generated 11/10/2006 4:22:46PM

A to Z Performance Components	Primary Contact	Secondary Contact
A to Z Performance Components	Tom Thompson	Bob Roberts
88 Lazy River Rd.	Office Manager	Office Manager
Atlanta, GA	Atlanta Office	Savannah Office
	Phone: 123 456-7890	Phone: 123 987-6543
Customer ID: 123-A004	Mobile: 123 654-0987	Mobile: 123 654-3678
Customer Criticality: 36.00	Email: tom.Thompson@perfcomp.com	Email: bob.Roberts@perfcomp.com

A to Z Customer Account Access SLA
Description - SLA for A to Z Performance Components provided by North East Data Solutions.

Configuration
SLA Created: 11/10/2006 9:52:21AM
SLA Never Expires
SLA Currently Active

Status For Recent SLA Periods

Unaffected
Compliant
Warned
Violated

Recent Periods

Warned	Nov 10 - Nov 11, 2006	Details	One or more guarantees exceeded it's warning threshold for this period.

A to Z Billing Service SLA
Description

Configuration
SLA Created: 11/10/2006 4:06:29PM
SLA Never Expires
SLA Currently Active

Status For Recent SLA Periods

Unaffected
Compliant
Warned
Violated

Recent Periods

Unaffected	Nov 1 - Dec 1, 2006	Details	- There were no impacted guarantees during this period.



Chapitre 8 : Assurance proactive des services

La solution de gestion des réseaux et de la voix de CA intègre des algorithmes permettant aux équipes chargées de l'exploitation d'identifier les zones de développement des problèmes au sein de l'infrastructure **avant** qu'ils n'aient une incidence sur le service client. Les problèmes se produisent rarement de manière instantanée. Des signes d'avertissement apparaissent souvent, tels que des détériorations discrètes mais grandissantes, une augmentation des erreurs et des retards. Ces problèmes peuvent être trop insignifiants pour être remarqués par les utilisateurs ou pour nécessiter des appels de service, mais ils se développent.

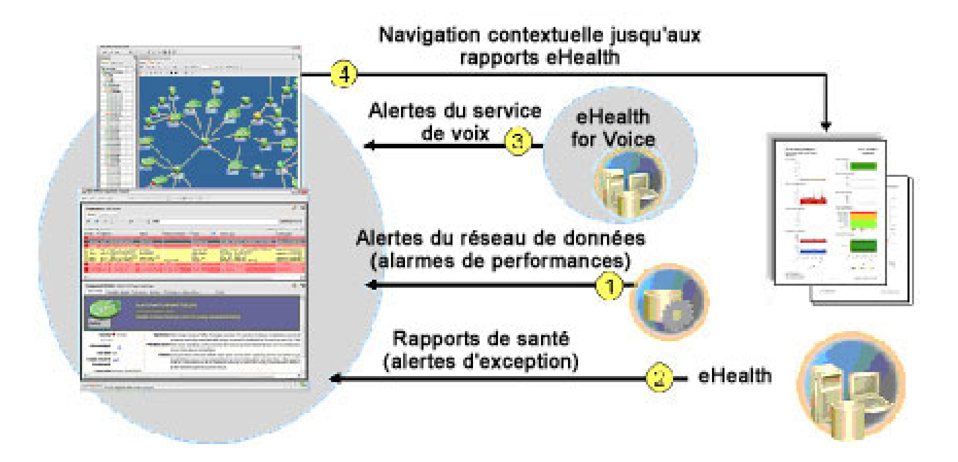
Grâce à des outils permettant d'analyser et de détecter le développement des problèmes et de déclencher des avertissements, les équipes chargées de l'exploitation peuvent régler les problèmes de façon proactive avant qu'ils n'entraînent des coupures et des interruptions ou des pertes de services. Cette fonctionnalité est particulièrement importante lors de l'implémentation des contrats de niveau de service. Si vous parvenez à résoudre les problèmes des contrats de niveau de service avant leur violation (sans recourir à d'autres ressources réseau et serveurs), vous pouvez économiser de l'argent et éviter des efforts inutiles.

Conditions préalables : les procédures du présent chapitre s'appuient sur l'hypothèse selon laquelle vous avez installé SPECTRUM et *e*Health et configuré Live Health de manière à pouvoir envoyer des traps à SPECTRUM. Pour plus d'informations sur la configuration de la solution intégrée, reportez-vous au chapitre 5. Pour obtenir des informations supplémentaires concernant l'application Live Health et la création de règles de surveillance, reportez-vous à l'aide en ligne de Live Health. L'aide en ligne d'*e*Health est installée sur le système *e*Health. Elle est également disponible sur le CD de documentation en ligne TotalDoc.

Identification des problèmes éventuels

L'analyse proactive de l'application *e*Health Live Health et l'analyse des exceptions de rapports de santé sont des outils clés qui vous avertissent du développement de problèmes sur votre réseau. Sur des réseaux convergents, *e*Health for Voice Policy Manager identifie le début des problèmes de voix et de messagerie. Tous ces outils fournissent des seuils et des paramètres configurables qui permettent de déterminer si un problème est suffisamment grave pour mériter une attention proactive.





Vous pouvez configurer ces outils de façon à observer le développement de ces problèmes et à envoyer des alarmes à SPECTRUM s'ils requièrent une attention particulière. De plus, vous pouvez configurer la durée du comportement avant de déclencher des alarmes, de manière à pouvoir réduire les fausses alarmes de simples violations de seuils et à vous concentrer sur les situations réelles incessantes.

Par exemple, l'application Live Exceptions de la gamme de produits Live Health fournit des notifications de retards, d'échecs et de problèmes de charge de travail inhabituelle potentiels sur les réseaux, les systèmes et les applications. Il utilise les données historiques regroupées et conservées par *e*Health pour évaluer les problèmes potentiels au fil du temps. Lorsque Live Exceptions détecte une condition méritant l'attention de l'opérateur, il déclenche une alarme et l'envoie à SPECTRUM.

Configuration de Live Health pour observer le développement des problèmes

Pour une assurance proactive des services, utilisez les algorithmes Time over Threshold et Deviation from Normal de Live Exceptions pour observer le développement des problèmes du service. Lorsque les performances sont anormales (en comparaison avec l'historique) sur une durée spécifique, Live Health déclenche une alarme et peut l'envoyer à SPECTRUM.

Pour configurer Live Health pour une assurance proactive des services :

1. Utilisez le navigateur Live Exceptions pour associer les profils de charge de travail inhabituelle par défaut à des groupes ou des listes de groupes de vos resources gérées. Utilisez l'outil de descriptions de profils Live Health sur http://support.concord.com/devices afin d'identifier les bons profils pour les types d'éléments que vous avez découverts. Pour plus d'informations sur l'association de profils à des groupes, reportez-vous au chapitre 5.

2. Si vous possédez des contrats de niveau de service personnalisés, vous pouvez créer des profils personnalisés avec des alarmes Time over Threshold et Deviation from Normal de manière à indiquer vos seuils de service. Assurez-vous que vos règles sont configurées de manière à vous avertir si les détériorations du service requièrent l'attention, ce qui correspond généralement à un seuil inférieur à vos seuils de contrats de service. Pour obtenir des instructions concernant la création de profils personnalisés, consultez l'aide en ligne de Live Health.



Configuration de rapports de santé pour envoyer des traps concernant le développement des problèmes

La section Exceptions d'un rapport de santé contient des informations sur les éléments ayant rencontré des événements inhabituels ou n'ayant pas de ressources suffisantes pour prendre en charge la demande qui leur est affectée. Cette section d'un rapport de santé identifie les éléments ayant accumulé un nombre important de points d'exception suite à des erreurs, à une forte utilisation et à une divergence par rapport aux tendances. Les éléments apparaissent dans le rapport uniquement lorsque leurs points d'exception accumulés sont supérieurs à un nombre minimum. Les administrateurs *e*Health peuvent spécifier ce nombre dans le profil de service du rapport.

Vous pouvez configurer les rapports de santé de manière à transférer des traps pour les exceptions Health au SpectroSERVER. Cela constitue un moyen supplémentaire de surveiller le service de manière proactive. Pendant l'exécution d'un rapport de santé planifié, *e*Health envoie un trap SNMP au SpectroSERVER concernant le problème principal de chaque élément dans la section Exceptions du rapport de santé. Le transfert de traps n'est pas activé par défaut sur *e*Health. Pour activer cette fonction, vous devez créer un rapport de santé personnalisé, puis planifier son exécution automatique.

Remarque : Seuls les rapports de santé planifiés transfèrent des exceptions. Ce n'est pas le cas des rapports exécutés manuellement.

Pour obtenir des instructions sur la création d'un rapport de santé personnalisé capable de transférer les exceptions en tant que traps à Live Health, reportez-vous au chapitre 5.

Envoi d'alertes vocales à SPECTRUM

*e*Health for Voice Release 4.0 propose l'intégration et la corrélation d'alarmes avec SPECTRUM, tout en tirant parti de SPECTRUM Service Management et de la capacité de modélisation de la voix. Vous pouvez configurer l'application *e*Health for Voice Policy Manager de manière à envoyer des traps SNMP à SPECTRUM en cas de non respect de la qualité des services ou de l'écoulement du trafic. SPECTRUM applique ses fonctions intelligentes aux stratégies, aux règles et aux modèles de manière à identifier la gravité du problème.

Policy Manager surveille l'intégralité de l'activité des données de la voix et des autocommutateurs privés, puis étudie ces données par rapport aux critères prédéfinis. Grâce à Policy Manager, vous pouvez définir des règles ou des stratégies relatives à tous types de données : modification de la configuration, trafic système, utilisation spécifique, alarmes, événements historiques, etc. Pour obtenir des instructions sur la configuration d'*e*Health for Voice de manière à envoyer des traps de performances à SPECTRUM, reportez-vous au chapitre 5.



Réponse à des actions d'alarme dans SPECTRUM

A l'aide de la console SPECTRUM OneClick, les opérateurs et les gestionnaires réseau peuvent visualiser les modèles (ou les ressources) dans leur topologie et observer les événements ou les modifications d'état indiquant le développement de problèmes sur leur réseau. Lorsque SPECTRUM reçoit un trap d'*e*Health, le modèle représentant l'élément change de couleur de manière à indiquer la gravité de l'alarme du trap reçu. Par exemple, en cas de problèmes critiques, l'icône du périphérique passe au rouge, alors que les problèmes mineurs la font passer au jaune.

Les opérateurs peuvent cliquer avec le bouton droit de la souris sur l'icône et effectuer les opérations suivantes pour résoudre ou rechercher les problèmes :

- Effectuer un zoom avant sur un rapport *e*Health Alarm Detail pour obtenir une illustration des tendances des performances provoquant la détection par Live Health de problèmes relatifs aux performances nécessitant le déclenchement d'une alarme. Par exemple, si un périphérique fonctionne en dehors des seuils de fonctionnement normaux pendant plus de 15 minutes, les rapports Live Health Alarm Detail peuvent indiquer la courbe de tendance des performances de l'élément.
- Exécuter un rapport *e*Health At-a-Glance ou Trend pour consulter l'historique des performances de la ressource. Alors qu'un rapport Trend indique les performances de la variable du problème spécifique, le rapport At-a-Glance présente un ensemble de variables communes des performances pour ce type d'élément. A l'aide de ces données, vous pouvez identifier les causes ou la racine du problème.
- Effacer l'alarme. Si l'opérateur sait que l'alarme correspond à une situation ou un problème connu, il peut l'effacer et rétablir le périphérique à l'état normal.
- Ouvrir les tickets Service Desk pour enregistrer le problème en tant que tâche de travail et l'affecter au personnel pour qu'il le règle. Grâce à l'intégration Unicenter Service Desk, SPECTRUM peut ouvrir, mettre à jour et fermer les tickets Service Desk de suivi du travail pour évaluer les problèmes sur le réseau. Les opérateurs travaillant au niveau de la console OneClick peuvent effectuer un zoom avant sur les détails des tickets Service Desk pour déterminer le dernier état et les personnes chargées de la résolution des problèmes.



Chapitre 9 : Planification prédictive de la capacité

La productivité des employés et la satisfaction des clients dépendent de la disponibilité et des performances des applications vitales. Les applications dépendent de l'infrastructure informatique exécutée normalement et de manière efficace.

Il ne suffit pas de résoudre les problèmes pour garantir que les ressources informatiques répondent aux besoins de vos utilisateurs. Pour une exécution efficace de votre infrastructure, vous devez obtenir des données concrètes concernant l'état actuel de votre réseau, identifier l'encombrement et les points sensibles avant qu'ils n'affectent les utilisateurs et faire des prévisions de manière efficace. Ces tâches font toutes partie de la planification prédictive de la capacité.

La planification de la capacité est une partie complexe et vitale de la gestion des ressources informatiques. Elle vous aide à utiliser vos ressources actuelles de manière efficace, à évaluer les tendances des exigences et à prévoir les futurs besoins en ressources. Une planification efficace de la capacité vous permet d'atteindre les objectifs suivants :

- Baisse des coûts grâce à la réduction ou l'élimination des lignes louées sous-exploitées
- Amélioration des performances grâce à l'identification des éléments sous-exploités et surexploités et rééquilibrage entre la capacité et la demande
- Réduction des temps d'arrêt du serveur et du réseau en anticipant les surcharges avant qu'elles ne se produisent et en garantissant la mise à disposition d'une capacité adéquate
- Amélioration de la prévisibilité du budget en suivant les tendances et en modélisant les effets de nouveaux services ou de nouvelles infrastructures, ce qui permet d'éviter les achats en urgence et de garantir l'obtention des meilleurs prix

Le présent chapitre explique comment *e*Health peut servir à effectuer quatre tâches majeures de planification de la capacité :

- Identification des ressources sous-exploitées de manière à trouver les ressources ou les périphériques correspondants qui provoquent des coûts inutiles pour les lignes louées et les systèmes inoccupés
- Identification des ressources surexploitées de manière à trouver les ressources ou les périphériques correspondants qui provoquent une altération des performances ou une augmentation des frais liés à la surexploitation
- Planification des futurs besoins en capacité en fonction des tendances actuelles de la demande ou des modifications métier prévues, ce qui permet de planifier les achats et d'installer des mises à niveau, le cas échéant
- Planification de la capacité vocale pour trouver les problèmes dus à la sous-exploitation ou à la surexploitation sur vos réseaux de télécommunication ou convergents.



Conditions préalables : si vous voulez suivre les recommandations de ce chapitre, votre base de données *e*Health doit contenir au moins une semaine de données collectées. Avec une plus grande quantité de données de performances et un historique plus long, ces rapports mettent mieux en évidence les tendances de la capacité et les problèmes d'utilisation.

Ces exemples partent également du principe selon lequel vous visualisez les rapports depuis l'interface Web d'*e*Health. Les rapports de l'interface Web possèdent des « points sensibles » interactifs, sur lesquels vous pouvez cliquer pour accéder à d'autres rapports et à des détails plus précis. Les zooms avant ne sont pas disponibles dans les rapports au format PDF.

Références supplémentaires : les procédures d'exécution, de planification et de personnalisation des rapports sont décrites en détail dans le manuel e*Health Report Management Guide* et sur l'aide en ligne d'*e*Health. Pour de plus amples informations sur les rapports *e*Health et sur leur fonctionnement, consultez l'aide en ligne d'*e*Health. Les recommandations de cette section sont extraites de la rubrique *Capacity Planning with* e*Health (Planification de la capacité avec* e*Health)*, disponible sur le site Internet *e*Health Support à l'adresse http://support.concord.com.

Identification des ressources sous-exploitées

Pour identifier les ressources sous-exploitées, procédez comme suit :

1. Localisez les ressources sous-exploitées.
2. Confirmez la sous-exploitation.
3. Traitez les ressources sous-exploitées.
4. Affichez le retour sur investissement.
5. Mettez à jour votre configuration.

Localisation des ressources sous-exploitées

*e*Health fournit un rapport Underutilized Elements (éléments sous-exploités) qui vous permet d'identifier rapidement les éléments susceptibles d'être sous-exploités. Ce rapport supplémentaire est en option dans les rapports de santé *e*Health. Pour le visualiser, vous devez personnaliser un rapport de santé et l'inclure.

Pour localiser les éléments sous-exploités de votre réseau :

1. Connectez-vous à l'interface Web d'*e*Health et sélectionnez l'onglet Run Reports.
2. Cliquez sur le lien Standard Health report. La page Run Health Report s'affiche.
3. Spécifiez le sujet des rapports (par exemple, technologie de réseau local/étendu et un groupe d'éléments).
4. Cliquez sur More Options et sélectionnez Supplemental sous Presentation Attributes.
5. Dans la liste de rapports Supplemental, sélectionnez Underutilized Elements pour inclure ce rapport.
6. Enregistrez le rapport sous un nom unique, par exemple Rapport_Sous-exploitation.



7. Cliquez sur Generate Report pour exécuter le rapport. L'exécution de ce rapport à la demande peut prendre plusieurs minutes. Nous vous recommandons de planifier l'exécution du rapport à partir de la console *e*Health de sorte que celui-ci soit exécuté la nuit ou à un moment où le système *e*Health n'est pas très occupé.

8. Consultez le rapport supplémentaire Underutilized Elements. Il répertorie les éléments répondant aux critères suivants sur les 8 derniers jours :

   › N'a jamais atteint 50 % d'utilisation

   › N'a pas atteint 10 % d'utilisation plus de 5 % du temps

9. Dans le rapport, recherchez les lignes louées, les routeurs, les commutateurs et les systèmes dont la bande passante, la capacité de l'UC, la mémoire ou l'espace disque sont sous-exploités. Par exemple, le rapport ci-dessous indique plusieurs lignes OC-3 haute vitesse faiblement utilisées. Il doit être examiné plus attentivement.

Underutilized Elements

			Element	
Rank	**Element Name**	**Speed**	**Type**	**Utilization Exception**
1	helium:-5734-ATM2/0	156.2 Mbs	ATM WAN Port	Underutilized Link, 99.00% of the baseline below 10% utilization (In)
2	helium:-5734-ATM2/0	156.2 Mbs	ATM WAN Port	Underutilized Link, 99.00% of the baseline below 10% utilization (Out)
3	helium:-5734-ATM3/0	156.2 Mbs	ATM WAN Port	Underutilized Link, 99.00% of the baseline below 10% utilization (In)
4	helium:-5734-LEC.1.13	156.2 Mbs	Generic LAN Interface	Underutilized Link, 99.00% of the baseline below 10% utilization (In)
5	helium:-5734-LEC.1.13	156.2 Mbs	Generic LAN Interface	Underutilized Link, 99.00% of the baseline below 10% utilization (Out)
6	helium:-7839-ATM0/0	155.5 Mbs	Generic WAN Interface	Underutilized Link, 99.00% of the baseline below 10% utilization (In)

Lorsque vous exécutez un rapport Underutilized Elements uniquement pour les éléments du réseau local/étendu, ces derniers sont d'abord triés en fonction de la vitesse (les liens du réseau étendu étant plus coûteux), puis en fonction du pourcentage de temps de sous-exploitation.

RECOMMANDATIONS

Lorsque vous utilisez le rapport Underutilized Elements, tenez compte des recommandations ci-dessous. Elles peuvent vous aider à rendre le rapport plus significatif pour votre environnement :

- Lors de la première installation d'eHealth, exécutez-le sur une base hebdomadaire de façon à identifier les ressources non exploitées. Après cette période initiale, vous pouvez l'exécuter moins souvent (chaque mois ou chaque trimestre) de manière à identifier les modifications d'exploitation sur votre réseau.
- Le rapport Underutilized Elements s'applique aux données des 8 derniers jours. C'est pourquoi vous devez planifier l'exécution le dimanche de manière à obtenir les données d'une semaine complète.
- En fonction de l'utilisation de votre réseau, vous pouvez modifier le profil des services pour que le rapport comprenne uniquement les données de certains jours ou de certaines heures, de façon à éliminer les périodes d'utilisation réduite du réseau (nuit, week-end, etc.).



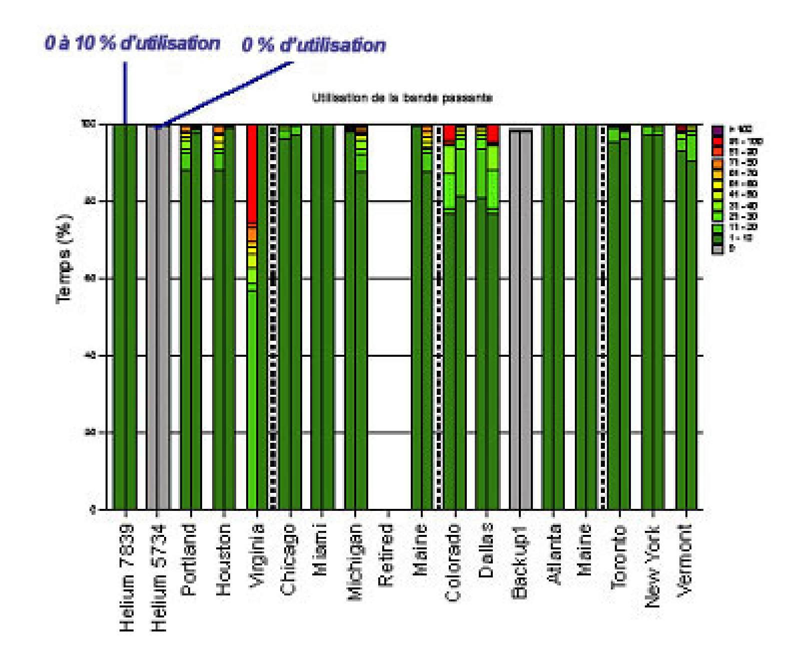
Confirmation de la sous-exploitation

Après avoir identifié les éléments sous-exploités, analysez la fonction de chaque élément et exécutez des rapports pour s'assurer de leur sous-exploitation réelle. Exécutez un rapport de santé mensuel pour confirmer que l'élément a été sous-exploité pendant au moins un mois.

Important : Vérifiez les liens réseau inutilisés pour déterminer s'ils constituent des sauvegardes. Les sauvegardes étant utilisées uniquement en cas d'échec du composant principal, elles ne sont souvent d'aucune utilité.

Pour confirmer la sous-exploitation d'un élément :

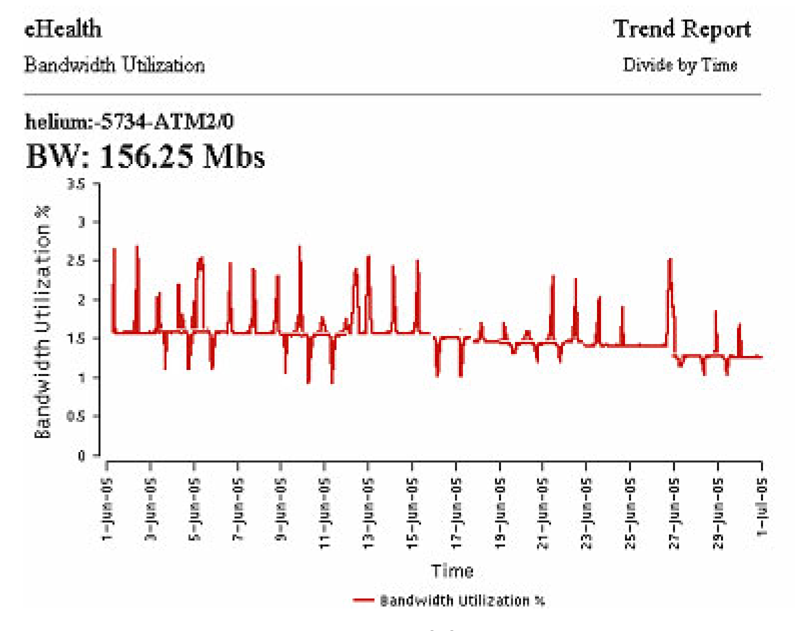
1. Dans le rapport de santé (tel que celui de la section précédente), examinez le graphique Bandwidth Utilization de la page Element Detail.



Le graphique Bandwidth Utilization représente la charge de chaque interface réseau sur la période du rapport. Par exemple, la barre représentant Helium 5734 est entièrement grise, ce qui indique que l'élément n'a pas été utilisé au cours du mois. Plusieurs autres barres, telles que celle représentant Helium 7839, Miami et Atlanta sont vert foncé, ce qui indique que ces composants n'ont jamais été utilisés à plus de 10 %. Toutes ces interfaces apparaissent comme sous-exploitées.



2. Exécutez un rapport Bandwidth Trend en cliquant sur la barre de l'élément que vous estimez sous exploité. Ce rapport indique l'utilisation de cet élément pour la même période que le rapport de santé.



3. Recherchez dans le graphique les éléments en sous-exploitation constante ou une diminution soudaine de l'utilisation due à la reconfiguration du réseau. Par exemple, l'élément ci-dessus n'a jamais été utilisé à plus de 3,5 % au cours du mois, ce qui indique qu'il est sous-exploité.
4. Etablissez un suivi du rapport pour apporter la preuve de cette exploitation réduite. En plus de ces rapports de santé hebdomadaires ou mensuels, vous pouvez exécuter un rapport Service Customer Service Level pour les données d'utilisation de la bande passante d'une durée plus longue (trimestriel ou annuel). Le rapport Service Customer contient également le graphique Daily Bandwidth Utilization, qui illustre en détail l'utilisation quotidienne.

Traitement des ressources sous-exploitées

Après avoir identifié et documenté les ressources sous-exploitées, envisagez les opérations suivantes pour traiter les problèmes d'utilisation :

- Supprimez les lignes sous-exploitées. Si une ligne louée est complètement inutilisée et ne sert pas de sauvegarde, vous pouvez la supprimer et économiser ainsi son coût mensuel.
- Rétrogradez les lignes sous-exploitées. Vous pouvez souvent réaliser des économies en rétrogradant la capacité du lien. Cette solution est efficace si le lien est de type T1 fractionnel, un circuit de relais de trame ou un canal ATM. Cependant, elle peut s'avérer compliquée si vous devez changer de technologie ou réaliser un nouveau câblage.
- Redirigez le trafic vers la ligne sous-exploitée. Si vous possédez des lignes surexploitées au même endroit ou des lignes pouvant être consolidées, redirigez le trafic du réseau vers une ligne sous-exploitée. Si vous ne possédez pas d'autre trafic à partir du même emplacement, envisagez les options suivantes :
    - Déplacez les serveurs locaux sur un site central pour augmenter le trafic sur la ligne sous-exploitée et réduire les coûts en consolidant le serveur.
    - Regroupez le trafic à partir de petites liaisons locales vers un centre régional, puis, à l'aide d'une liaison haute vitesse partagée, vers le site central.



Affichage du retour sur investissement

Après avoir déterminé les modifications à apporter à la capacité, vous pouvez calculer et afficher les économies mensuelles potentiellement réalisées grâce à l'élimination de lignes et à la différence de coût entre les lignes existantes et les nouvelles lignes rétrogradées.

Pour estimer le retour sur investissement :

1. Examinez les frais d'utilisation mensuels pour déterminer le coût des lignes louées pouvant être sous-exploitées.

2. Contactez votre fournisseur de services pour définir les coûts possibles de la modification de services ainsi que les nouveaux coûts mensuels des modifications de la vitesse ou de la bande passante. Si vous avez des coûts internes relatifs à la modification de services, prenez-les également en compte.

3. Calculez le retour sur investissement des modifications effectuées à l'aide de l'équation ci-dessous :

   Retour sur investissement = modification des coûts / économies mensuelles

   Le tableau ci-dessous illustre les coûts et frais de service pour trois interfaces :

	Net-Link	Chicago T1	Paxton T1
Vitesse actuelle	100 Mbits/s	1,54 Mbits/s	1,54 Mbits/s
Nouvelle vitesse	10 Mbits/s	512 Kbits/s	128 Kbits/s
Coût actuel	3 300 dollars	2 500 dollars	5 000 dollars
Nouveau coût	2 500 dollars	2 000 dollars	3 200 dollars
Coût du changement	5 000 dollars	1 000 dollars	1 200 dollars
Economies mensuelles	800 dollars	500 dollars	1 800 dollars

4. En fonction de vos calculs de retour sur investissement, déterminez l'intérêt des modifications proposées. Par exemple, le tableau indique que la rétrogradation de l'interface Net-Link d'une ligne 100 Mbits/s à une ligne 10 Mbits/s vous permettrait d'économiser 800 dollars tous les mois, mais le coût de changement élevé signifie que vous ne feriez pas d'économies, même sur plus de six mois. En revanche, la rétrogradation de l'interface Paxton T1 à une ligne 128 Kbits/s vous permettrait d'effectuer un retour sur investissement en moins d'un mois.



Mise à jour de votre configuration

Après avoir modifié votre configuration pour résoudre les problèmes liés à la capacité, mettez à jour vos environnements SPECTRUM et *e*Health pour vous assurer qu'ils tiennent compte des vitesses mises à jour et éventuellement des ressources ayant été supprimées.

Pour mettre votre configuration à jour :

1. Mettez à jour vos vues SPECTRUM en effectuant une nouvelle découverte afin de vérifier qu'elles tiennent compte des informations de périphérique les plus récentes.

2. Mettez à jour la configuration de l'interrogation *e*Health et les listes d'éléments en réimportant les informations des éléments à partir de SPECTRUM et en effectuant une nouvelle découverte de vos éléments. Il se peut que les rapports ultérieurs des plages horaires relatives aux modifications de vitesse des éléments affichent des pourcentages d'utilisation inhabituels.

3. Si vous avez réduit la capacité ou accru la demande des ressources existantes, exécutez des rapports de tendance et de santé sur ces ressources. Recherchez les exceptions Health ou autres problèmes d'utilisation pouvant provenir de l'augmentation du trafic.

4. Si vous avez éliminé un élément, désactivez l'interrogation et supprimez l'élément de la base de données *e*Health. La suppression de l'élément vous permet de continuer à générer des rapports sur celui-ci jusqu'à ce que les données le concernant soient trop anciennes pour être conservées dans la base de données.

Identification des ressources surexploitées

Pour identifier les ressources surexploitées, procédez comme suit :

1. Localisez les ressources surexploitées.

2. Confirmez la surexploitation.

3. Traitez les ressources surexploitées.

Localisation des ressources surexploitées

Les outils de planification de la capacité d'*e*Health peuvent vous aider à identifier les ressources surexploitées avant qu'elles ne commencent à être problématiques. En examinant un seul rapport de santé par semaine, vous pouvez identifier les éléments du réseau qui atteignent leur capacité. Vous pouvez alors consulter d'autres rapports pour analyser les problèmes et les résoudre avant qu'ils ne deviennent insurmontables pour votre équipe informatique.



Pour localiser les ressources surexploitées :

1. Sur l'interface Web d'eHealth, exécutez un rapport de santé quotidien pour le jour le plus chargé de la semaine.

2. Dans le volet gauche de la fenêtre du rapport de santé, cliquez sur Exceptions Summary pour ouvrir le rapport du même nom. Le rapport Exceptions Summary identifie les éléments ayant rencontré des événements inhabituels ou dont les ressources sont constamment inadaptées à la demande qui leur est affectée. Les éléments sont classés par points d'exception, de manière à ce que ceux qui rencontrent les problèmes les plus graves soient répertoriés en premier.

Exception Summary Report

			Element	Ranking	Total	
Rank	Element Name	Speed	Type	Points	Exceptions	Leading Exception
1	Virginia	512 Kbs	Frame Relay	171.1	2	Utilization Health Index
2	Dallas-Houston	128 Kbs	Frame Relay	96.6	2	Utilization Health Index
3	Colorado	56 Kbs	Frame Relay	85.2	2	Congestion Health Index

3. Dans le rapport, recherchez les éléments qui répertorient Utilization Health Index ou Congestion Health Index dans la colonne Leading Exception. Ces éléments ont un volume important et peuvent être surexploités.

   Par exemple, le lien Frame Relay vers le bureau de Virginie est répertorié en premier. Son exception principale est Utilization Health Index. Ce lien est vraisemblablement surexploité et doit être examiné plus attentivement.

Confirmation des ressources surexploitées

Le graphique Situations to Watch identifie les éléments censés dépasser, atteindre ou approcher leurs seuils de tendance. Il indique l'écart de chaque élément par rapport à son seuil, la vitesse d'augmentation de l'utilisation et le temps restant avant que la demande ne dépasse la capacité.

Pour confirmer la surexploitation des ressources :

1. Dans l'interface Web d'eHealth, exécutez un rapport de santé pour la semaine précédente.

2. Consultez le graphique Situations to Watch dans la section Summary du rapport de santé.

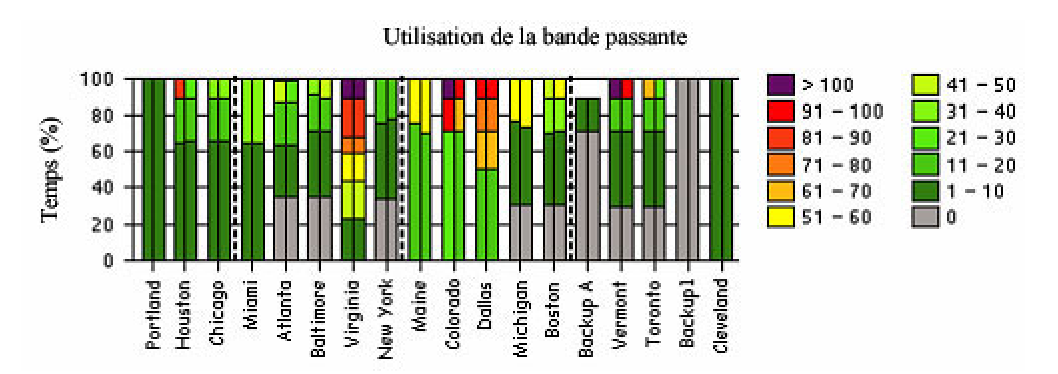
Situations à surveiller

			Seuil	Moyenne quotidienne		Jours jusqu'à (depuis)
Rang	Nom de l'élément	Variable	Valeur	Réelle	Prévue	Seuil
1	Virginia (In)	Volume (Bandwidth %)	100.00	114.9	113.3	(2)
2	Dallas (Out)	Congestion (ppm Frames)	1000.00	908.5	908.2	1
3	Colorado (In)	Volume (Bandwidth %)	100.00	88.5	88.2	7
4	Maine (Out)	Volume (Bandwidth %)	100.00	8.5	3.3	Increasing
5	Michigan (Out)	Congestion (ppm Frames)	1000.00	188.5	114.2	Increasing



3. Consultez les éléments répertoriés dans le graphique et recherchez ceux qui ont dépassé leur seuil ou dont la croissance est assez rapide pour qu'ils l'atteignent bientôt. Par exemple, le premier élément (Virginia) dépasse déjà le seuil depuis deux jours, alors qu'il est prévu que les deux suivants atteignent leurs seuils au coursde la semaine prochaine. Tous ces éléments sont vraisemblablement surexploités. La demande concernant les deux derniers éléments répertoriés augmente, mais ils sont tous deux encore en dessous de 20 % de capacité. Ils ne constituent donc pas un problème.

4. Dans le rapport de santé, sélectionnez Element Detail et examinez le graphique Bandwidth Utilization pour les éléments que vous pensez être surexploités.



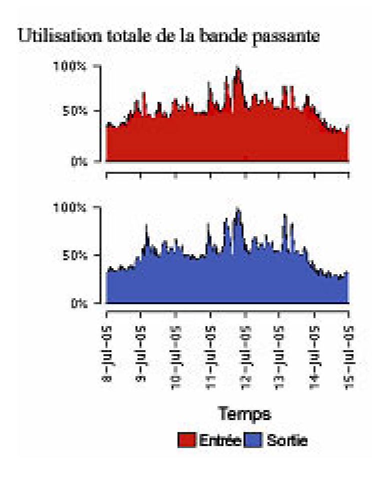
Le graphique Bandwidth Utilization indique le pourcentage du temps de chaque élément dans chaque plage d'utilisation. Généralement, le violet et le rouge indiquent une ressource surexploitée. Le violet représente une utilisation supérieure à 100 %, ce qui signifie que l'élément est probablement une ligne louée dépassant la bande passante contractuelle et, de plus, engageant des frais supplémentaires.

5. Examinez le graphique pour connaître le nombre de fois où un élément suspecté a été surexploité au cours de la semaine. Certains éléments peuvent afficher une forte demande constante (comme la ligne Virginia), mais étant donné que la demande varie dans le temps, la plupart des éléments affichent de longues périodes d'utilisation réduite. Selon l'activité de votre réseau, un élément peut être inutilisé à certaines heures (par exemple, la nuit), mais être quand même surexploité car la demande dépasse la capacité aux heures d'utilisation maximale.

   Par exemple, dans le graphique, la ligne Vermont n'indique aucune utilisation pendant un tiers du temps (peut-être la nuit) et est utilisée à moins de 20 % la plupart du temps. Cependant, puisqu'elle est utilisée à plus de 100 % lorsque la demande est maximale, elle pourrait engager des frais supplémentaires et être ainsi considérée comme surexploitée.



6. Pour obtenir des informations supplémentaires sur les performances d'un élément, créez un rapport At-a-Glance en cliquant sur cet élément dans le graphique Bandwidth Utilization.



7. Consultez les graphiques Bandwidth Utilization dans le rapport At-a-Glance pour déterminer la fréquence et les périodes de surexploitation de l'élément. Les exemples de graphiques indiquent que l'élément a été utilisé à 50 % la majeure partie de la semaine, mais que son utilisation maximale a pratiquement atteint 100 % à plusieurs reprises. En fonction de vos besoins métier, un élément qui atteint sa capacité Durant une heure par semaine seulement peut être acceptable, mais une heure de surexploitation peut devenir un problème critique si elle survient à une période de fonctionnement clé.

8. Recherchez toute anomalie dans les autres graphiques du rapport At-a-Glance, y compris les taux d'erreur élevés ou les signes d'encombrement (notifications explicites d'encombrement vers l'avant ou vers l'arrière, rejets, etc.). Utilisez ces informations pour déterminer les conditions pouvant affecter l'élément, telles que :

   - Capacité insuffisante
   - Applications inefficaces ou mal configurées consommant trop de bande passante
   - Nombre trop important ou insuffisant de postes surchargeant un lien de réseau étendu
   - Domaine fortement répété ou dupliqué à diriger

9. Etablissez un suivi du rapport pour apporter la preuve d'une utilisation intensive. En plus des rapports décrits ici, vous pouvez sélectionner des éléments spécifiques dans le rapport Exceptions Summary et le graphique Situations to Watch afin d'exécuter des rapports détaillés. Vous pouvez également exécuter des rapports Bandwidth Trend sur des éléments spécifiques pour montrer l'utilisation d'une ressource sur le long terme.

Traitement des ressources surexploitées

Après avoir identifié et documenté les ressources sous-exploitées, envisagez d'effectuer les opérations suivantes pour résoudre le problème :

- Mettez à niveau l'élément vers une capacité supérieure.
- Déplacez la demande vers d'autres ressources.
- Ajoutez des éléments pour partager la charge de travail.

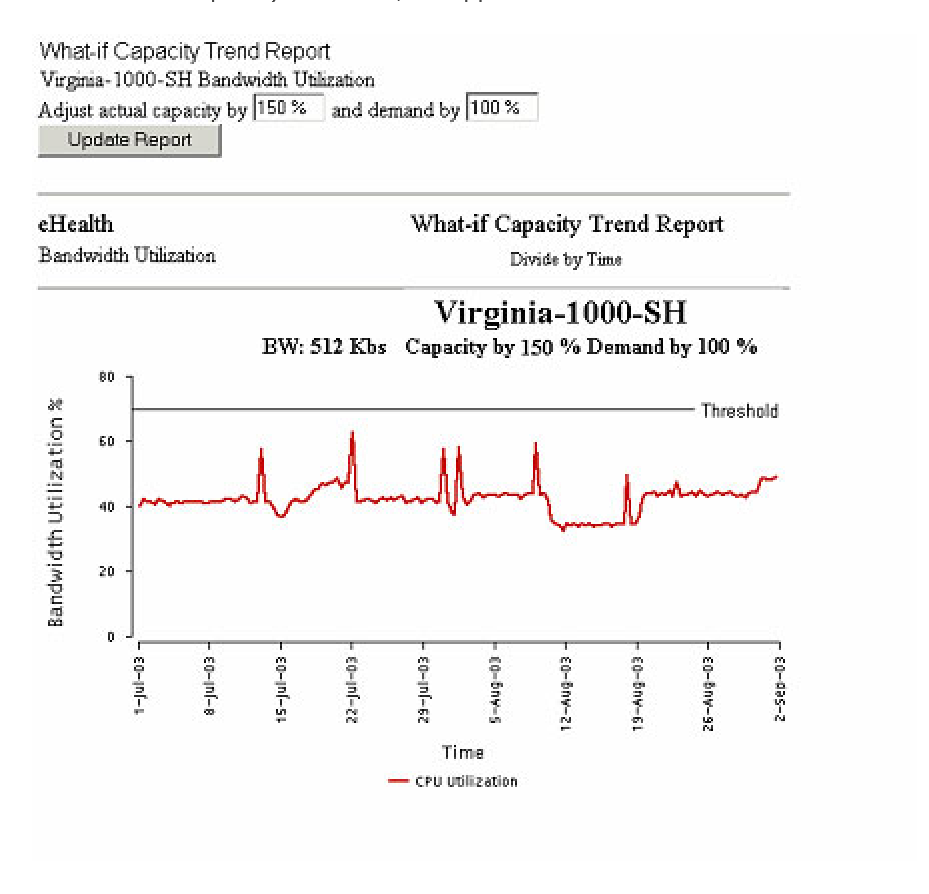


RECOMMANDATION

Utilisez les rapports Capacity Trend What-If pour visualiser les effets d'une capacité supérieure ou d'une demande moins importante sur l'élément surexploité et déterminer la capacité optimale de toute nouvelle ressource. Lorsque vous exécutez le rapport, vous spécifiez un élément, une variable de capacité et une plage horaire. Le rapport indique la valeur de la variable de performances pendant cette plage historique.

Le rapport What-If ressemble beaucoup au rapport Trend d'*e*Health. Cependant, vous pouvez modifier la capacité de la ressource, la demande placée sur la ressource à cette période ou les deux. Mettez ensuite à jour le rapport pour modéliser les effets des modifications possibles.

Remarque : Lorsque vous définissez la capacité et la demande, veillez à spécifier des valeurs en pourcentage. Par exemple, 100 % indique que le rapport utilise les valeurs actuelles. A 50 %, le rapport affiche la moitié des valeurs actuelles (en divisant la capacité ou la demande par 2). A 200 %, le rapport double les valeurs actuelles.



Ce rapport montre que l'augmentation de 50 % de la capacité de la ligne Virginia (capacité = 125 %) entraîne une réduction de l'utilisation maximale à environ 60 % de la capacité. Cette capacité doit être suffisante pour répondre à la demande attendue.



Planification des modifications futures de la capacité

Pour planifier et prévoir les modifications de la capacité, suivez la procédure ci-dessous :

1. Identifiez les modifications éventuelles de la capacité.
2. Analysez les tendances de la capacité.
3. Visualisez les modifications de la capacité.
4. Traitez les modifications de la capacité.

Identification des modifications éventuelles de la capacité

*e*Health fournit des rapports de planification de la capacité vous permettant d'analyser le comportement de vos ressources dans différentes conditions et de prévoir où et quand vous aurez besoin d'ajouter de la capacité.

Pour identifier les problèmes de capacité éventuels :

1. Planifiez l'exécution d'un rapport de santé tous les dimanches pour garantir l'obtention des données pour la semaine complète. Pour obtenir les instructions, reportez-vous à la section concernant la personnalisation et la planification de rapports de santé au chapitre 5 du présent manuel.

2. Dans la section Summary du rapport de santé, examinez le graphique Situations to Watch. Ce graphique affiche les 10 premiers éléments (interfaces réseau, UC, partitions de disque) approchant leur seuil de capacité. Il indique l'écart de chaque élément par rapport à son seuil, la vitesse d'augmentation de l'utilisation et le temps restant avant que la demande ne dépasse la capacité.

Situations à surveiller

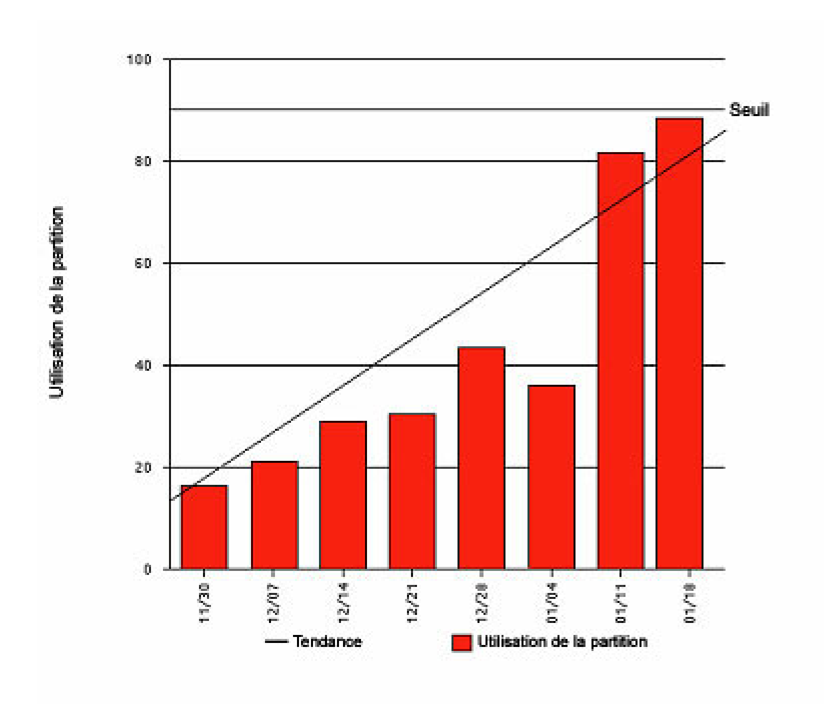
			Seuil	Moyenne hebdomadaire		Jours jusqu'à (depuis)
Rang	Nom de l'élément	Variable	Valeur	Réelle	Prévue	Seuil
1	System-Orange	Partition Utilization	90.000	88.663	90.191	0
2	System-Green	Partition Utilization	90.000	82.012	81.942	20
3	System-Purple	Partition Utilization	90.000	41.202	46.580	80
4	System-Black	Virtual Memory Utilization	90.000	40.000	43.469	86
5	System-White	Partition Utilization	90.000	70.620	71.686	144
6	System-Pink	Partition Utilization	90.000	45.746	47.685	Increasing
7	System-Brown	Partition Utilization	90.000	41.620	40042	Decreasing

Ce rapport indique plusieurs partitions utilisateur approchant leurs seuils. Dans la colonne Days To Threshold, System-Orange affiche 0, ce qui signifie que l'utilisation a atteint le seuil de tendance. System-Green indique 20 jours jusqu'au seuil et System-Pink affiche Increasing, ce qui indique une augmentation de l'utilisation, mais insuffisante pour atteindre le seuil pendant une longue période.



Chaque système qui atteint ou se rapproche de son seuil nécessite un examen plus approfondi. Par exemple, il se peut que System-Orange soit déjà surexploité ou qu'il s'agisse d'une partition système conçue pour fonctionner à un niveau proche de sa capacité. D'autre part, System-Green requiert encore 20 jours pour atteindre son seuil, mais il peut être intéressant de le mettre à niveau s'il montre une augmentation stable de la demande.

3. Pour obtenir de plus amples informations sur chaque situation spécifiée, cliquez sur le nom de l'élément afin d'exécuter un rapport Situations to Watch Detail de la partition.



4. Examinez la courbe de tendance pour déterminer la vitesse à laquelle la tendance se rapproche du seuil. Si la courbe monte de manière constante, comme dans cet exemple, vous pouvez ajuster la capacité en augmentant la taille de la partition, en supprimant les répertoires et fichiers inutiles ou en achetant un nouveau système.

Analyse des tendances de la capacité

Après avoir identifié les candidats éventuels à une mise à niveau, exécutez des rapports Capacity Projection et Capacity Provisioning pour prévoir les modifications du volume sur les semaines et les mois à venir, ainsi que la période à laquelle les éléments auront besoin d'être mis à niveau.

Pour exécuter des rapports Capacity Projection et Capacity Provisioning :

1. Connectez-vous à l'interface Web d'eHealth et sélectionnez l'onglet Run Reports.

2. Cliquez sur le lien Standard Health report. La page Run Health Report s'affiche.

3. Spécifiez le sujet des rapports (par exemple, technologie système et un groupe d'éléments).



4. Cliquez sur More Options et effectuez les opérations suivantes :

   a. Sous Presentation Attributes, sélectionnez Capacity.

   b. Sélectionnez Capacity Projection et Capacity Provisioning pour ces rapports.

   c. Spécifiez 20 dans le champ Capacity Provisioning Minimum Lead-Time.

   d. Spécifiez 90 dans le champ Capacity Provisioning Maximum Lead-Time.

5. Enregistrez le rapport en tant que modèle sous un nom unique, tel que Rapport_Capacité.

6. Cliquez sur Generate Report pour exécuter le rapport. L'exécution du rapport à la demande peut prendre quelques minutes. Il est recommandé de planifier l'exécution du rapport à partir de la console *e*Health pour que celui-ci soit généré automatiquement pendant les heures d'utilisation réduite et qu'il soit prêt à être consulté lorsque vous en avez besoin.

7. Consultez le rapport Capacity Projection. Le rapport prévoit les modifications ultérieures de la capacité d'une variable spécifique (par exemple, l'utilisation de la partition). Vous pouvez exécuter le rapport en fonction des valeurs de capacité maximales, moyennes ou centiles. *e*Health mesure les valeurs de capacité prévues par rapport à un seuil spécifié par l'utilisateur et affiche les éléments censés dépasser le seuil.

Projection de la capacité de la partition

	Seuil	Moyenne hebdomadaire			
Nom de l'élément	Valeur	Réelle	30 jours	90 jours	9 mois
System-Orange	90.000	88.663	88.686	90.063	90.580
System-Green	90.000	82.012	90.042	90.932	90.520
System-Purple	90.000	41.202	41.202	90.000	90.101
System-White	90.000	70.620	70.620	71.686	90.167
System-Pink	90.000	45.746	45.963	55.746	60.000
System-Brown	90.000	41.620	41.020	40.000	40.000

Ce rapport affiche le pourcentage de capacité de la partition consommée sur chaque système au bout de 30 jours, 90 jours et sur les neuf mois à venir. Vous pouvez constater que la demande sur System-Orange est proche du seuil, mais qu'elle n'augmente pas beaucoup. En revanche, la demande sur System-Purple augmente rapidement et dépassera bientôt le seuil de capacité. Il se peut donc que System-Purple ait le plus besoin d'une mise à niveau.



8. Pour prévoir le moment où ces éléments auront besoin d'une mise à niveau, consultez le rapport Capacity Provisioning. Le rapport Capacity Provisioning compare les valeurs de capacité prévues par rapport à un seuil de mise à niveau et affiche les éléments censés dépasser le seuil, ainsi que le nombre de jours restants jusqu'à ce qu'une mise à niveau soit nécessaire.

Prévision de la capacité avec délai d'exécution de 20 à 90 jours, point de mise à niveau de 90 %

		Moyenne quotidienne	Jours jusqu'à
Nom de l'élément	Variable	Réelle	Mise à niveau
System-Green	Utilisation de la partition	82.012	20.00
System-Purple	Utilisation de la partition	41.202	80.00
System-Black	Virtual Memory Utilization	40.000	86.00

Comme pour le rapport Capacity Projection, vous pouvez exécuter ce rapport en fonction des valeurs de capacité maximales, moyennes ou centiles. Vous pouvez définir le seuil de mise à niveau ainsi qu'une fenêtre de délai d'obtention de mise à niveau en personnalisant les attributs Presentation Attributes du rapport de santé.

Le rapport indique les éléments censés atteindre un niveau égal à 90 % de la capacité dans les 20 à 90 prochains jours. System-Green représente la mise à niveau la plus nécessaire et doit être traité dans les 20 jours.

RECOMMANDATIONS

Pour les rapports Capacity Projection et Provision, il est important de connaître le délai d'exécution requis pour remettre en ligne de la capacité. Par exemple, certains fournisseurs de service peuvent avoir besoin de 90 jours pour fournir une nouvelle ligne T1. Dans le cas des systèmes, 30 jours peuvent être nécessaires pour commander et ajouter de la mémoire ou de l'espace disque supplémentaire. Par conséquent, selon les types de ressources que vous gérez, vous devez savoir à quel moment commander de la capacité supplémentaire pour qu'elle soit disponible (avant d'atteindre le moment de mise à niveau).

Ces rapports identifient les emplacements pour lesquels de la capacité supplémentaire doit être commandée immédiatement pour éviter d'atteindre le seuil. Les exemples de cette section montrent un délai d'exécution de 20 à 90 jours. Les trois emplacements sont prévus pour nécessiter une mise à niveau dans cette fenêtre. S'il faut 90 jours pour ajouter de l'espace disque ou de la mémoire, il est fort probable que 90 % du seuil de la mise à niveau ne soient pas respectés au cours de cette période. La première fois que vous utilisez *e*Health pour surveiller vos ressources, il est possible que certaines d'entre elles aient besoin d'être mises à niveau plus tôt que ne le permettent les délais d'exécution. Mais dans le temps, ces rapports vous aident à isoler les problèmes plus rapidement et à éviter les violations de seuil avant expiration de la fenêtre de délai d'exécution.

Visualisation des modifications de la capacité

Le rapport Capacity Trend What-If montre de quelle manière les ressources agissent au fur et à mesure que votre infrastructure se modifie et se développe. Ces rapports permettent d'exploiter des données historiques afin de prévoir les futurs modèles, les modifications de modèles de capacité ou de demande et de déterminer l'effet sur les ressources.



Pour simplifier la visualisation de l'impact des modifications de la demande :

1. Exécutez un rapport Capacity Trend What-If pour analyser les éventuelles solutions :

    a. Sur la page On the Run Reports, dans la colonne Available Reports sous What-If, sélectionnez CapacityTrend ou un autre nom de modèle. La page Run a Capacity Trend What-If Report apparaît.

    b. Sélectionnez un type d'élément dans la liste Element Type, puis sélectionnez un élément dans liste Available elements.

    c. Sélectionnez une variable pour votre rapport.

    d. Sous Chart type, sélectionnez le format de graphique.

    e. Sous Divide by, spécifiez un type de représentation graphique pour la variable sélectionnée.

    f. Si vous le souhaitez, sélectionnez un intervalle de temps au cours duquel les données sont cumulées.

    g. Sélectionnez une taille d'échantillon en fonction de la plage horaire de votre rapport. La taille d'échantillon As Is utilise les données les plus granulaires disponibles et ne cumule pas les valeurs.

    h. Sous Report Time, sélectionnez la période du rapport. Vous pouvez spécifier les valeurs immédiatement, aujourd'hui, demain ou hier, ou encore une date réelle ou une valeur de temps.

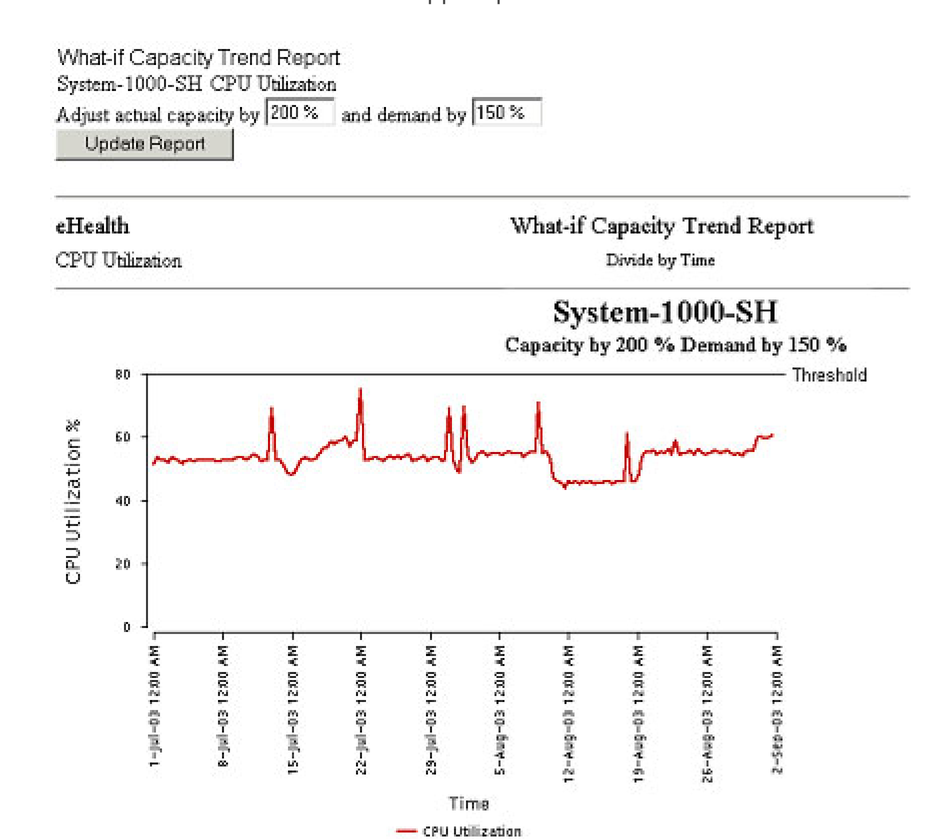
    i. Sélectionnez More Options pour spécifier les heures et les jours d'apparition du rapport.

    j. Si vous le souhaitez, vous pouvez personnaliser le rapport en définissant des attributs de présentation.

    k. Cliquez sur Generate Report.



2. Utilisez les champs en haut du rapport pour ajuster la capacité et/ou la demande de ressource et réexécuter le rapport pour modéliser la modification.



3. Utilisez le rapport pour effectuer la modélisation et pour déterminer si une ressource existante peut prendre en charge des modifications anticipées et si tel n'est pas le cas, la quantité de capacité pouvant être ajoutée. Vous pouvez également illustrer les problèmes potentiels, de manière à pouvoir émettre des requêtes pour un nouvel équipement ou des mises à niveau.

   Par exemple, ce rapport montre qu'en doublant la capacité de l'UC, la demande sur le serveur est bien inférieure au seuil de tendance de 80 %, même avec une hausse de 50 % de la demande.

Traitement des modifications de la capacité

Après avoir identifié les améliorations ou les problèmes de capacité possibles, étudiez les actions suivantes pour résoudre le problème :

- Mettez à niveau l'élément vers une capacité supérieure.
- Remplacez l'élément par un périphérique plus grand ou plus rapide, tel qu'un disque plus volumineux, une interface ou une UC plus rapide.

Le rapport What-If peut vous aider à modéliser ou à visualiser la manière dont les changements suggérés vont améliorer les performances. Après toute modification des périphériques ou des ressources, mettez à jour votre configuration comme décrit dans le chapitre 5.



Planification de la capacité vocale

Pour les réseaux dotés de périphériques de téléphonie classiques ou de voix sur IP ou pour les systèmes de messagerie vocale, *e*Health for Voice peut vous aider à identifier les problèmes de capacité et à surveiller la qualité d'écoulement du trafic pendant les heures de pointe du réseau. Dans le cas des périphériques de voix, les problèmes de capacité peuvent comprendre l'utilisation des jonctions/ports et l'espace disque de la messagerie vocale. Lorsque ces facteurs sont surexploités, les services et la satisfaction des clients sont dégradés. Lorsque ces facteurs sont sous-exploités, il est important d'identifier l'endroit où les périphériques risquent d'être surapprovisionnés, de manière à pouvoir réduire les coûts et réaffecter les ressources, afin de résoudre l'encombrement sur d'autres zones du réseau.

Une planification efficace de la capacité vous permet d'atteindre les objectifs suivants :

- Baisse des coûts grâce à la réduction ou à l'élimination des lignes louées sous-exploitées et à la réduction des frais de maintenance des ports non utilisés ou inutiles
- Amélioration des performances en identifiant les ports ou les jonctions surexploités ou sous-exploités et en rééquilibrant la capacité et la demande
- Amélioration de la prévisibilité budgétaire en suivant les tendances, ce qui contribue à éviter les achats d'urgence et à assurer la recherche et la prévision des meilleurs coûts de service

Pour comprendre les modèles de trafic, vous devez collecter à partir de l'autocommutateur privé des informations qui détaillent le trafic de pointe de chaque groupe de jonctions, sur quelques semaines et, de préférence, sur quelques mois. Ces informations sont disponibles au niveau de la commutation. *e*Health for Voice automatise la collecte de ces informations, ce qui facilite l'exécution d'évaluations de maintenance trimestrielles et à la demande de la capacité vocale et des modèles d'utilisation.

Analyse de la capacité vocale

Après avoir collecté les informations sur le trafic de la période voulue, vous pouvez utiliser l'outil Capacity Analyzer pour déterminer le niveau de satisfaction client offert par vos périphériques de voix pendant les heures de pointe. A partir de cette boîte de dialogue, vous pouvez rapidement calculer la qualité d'écoulement du trafic, visualiser la capacité de l'espace disque pour les serveurs de messagerie et visualiser la capacité de traitement des serveurs de communications.

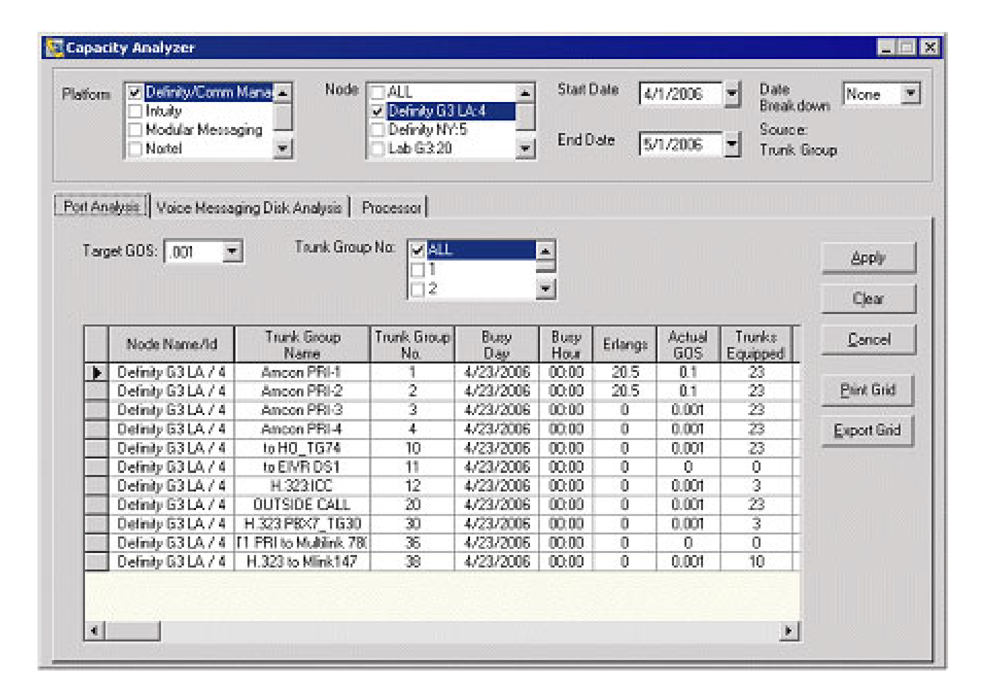


Pour accéder à Capacity Analyzer :

1. Sur le système sur lequel *e*Health for Voice est installé, sélectionnez Démarrer, Programmes, *e*Health for Voice, *e*Health for Voice. La console de programmation *e*Health for Voice s'affiche.

2. Dans l'arborescence gauche de la console de navigation, sélectionnez Measurements, Reports.

3. Dans le volet droit de la console, double-cliquez sur l'icône Capacity Analyzer. La boîte de dialogue Capacity Analyzer apparaît.



Analyse de la qualité d'écoulement du trafic

*e*Health for Voice calcule la qualité d'écoulement du trafic pour déterminer le niveau de service offert aux appelants (appels répondus, occupé ou sonnerie sans réponse) pendant les heures de pointe de la période. Cela permet de déterminer la bande passante supplémentaire nécessaire pour transporter le trafic de voix sur le réseau.

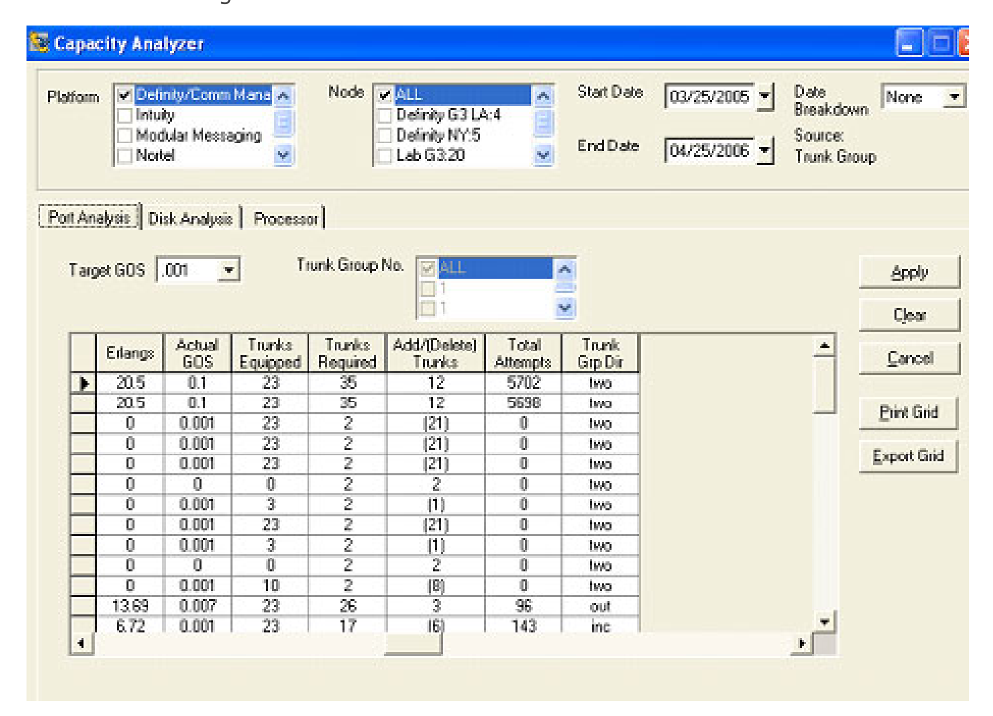
Pour analyser la qualité d'écoulement du trafic :

1. Dans la boîte de dialogue Capacity Analyzer, sélectionnez l'onglet Port Analysis pour accéder à l'outil de calcul de la qualité d'écoulement du trafic. La qualité d'écoulement du trafic cible correspond au pourcentage d'appelants servis (appels répondus) pendant l'heure la plus chargée. Une qualité d'écoulement du trafic de 0,001 signifie que 0,999 % des appelants sera traité.

2. Sélectionnez la qualité d'écoulement du trafic cible et cliquez sur Apply. La boîte de dialogue montre le nombre de jonctions à ajouter pour prendre en charge la qualité d'écoulement du trafic.



3. Utilisez la barre de défilement horizontale pour vous déplacer dans la partie droite de la boîte de dialogue.



4. Consultez la colonne Add/(Delete) Trunks pour déterminer le nombre de jonctions à fournir pour cette qualité d'écoulement du trafic. Un nombre entre parenthèses indique le total de jonctions que vous pouvez supprimer et pouvant prendre en charge la qualité d'écoulement du trafic pendant les heures de pointe, ce qui vous aide à détecter les ressources sous-exploitées.
5. Consultez la colonne Erlangs pour déterminer le trafic de pointe réel. Un Erlang est une mesure de la capacité du trafic de voix. Il représente le nombre de minutes de trafic de voix pendant une heure. Si au cours d'une heure, 10 utilisateurs passent chacun un appel de 10 minutes, l'heure contient 100 minutes d'appels et 1,67 Erlangs de trafic. Ces informations vous aident à identifier la quantité de bande passante supplémentaire requise sur le réseau pour prendre en charge la voix.

RECOMMANDATIONS

Lorsque vous utilisez l'outil Capacity Analyzer, tenez compte des recommandations suivantes pour améliorer les résultats dans votre environnement :

- A la première installation d'eHealth for Voice, exécutez chaque semaine l'outil Capacity Analyzer pour identifier les ressources inutilisées. Après cette période initiale, vous pouvez l'exécuter moins souvent (chaque mois ou trimestre) pour identifier les modifications d'utilisation sur le réseau.
- Les lignes de jonction ou de port avec un trafic très faible ou nul peuvent correspondre à des sauvegardes ou à des lignes de dépassement. Avant de poursuivre avec les plans de modification de services détaillés, consultez toujours le technicien chargé des autocommutateurs/ autocommutateurs IP pour vous assurer que vous comprenez bien la fonction de chaque jonction et port.
- Le niveau de surexploitation ou de sous-exploitation varie en fonction de la qualité d'écoulement du trafic sélectionné. Plus la qualité d'écoulement du trafic diminue, plus le besoin en ressources supplémentaires augmente. Les niveaux de service des entreprises permettent de définir la qualité d'écoulement du trafic requise dans votre environnement.



Traitement des ressources sous-exploitées

Après avoir identifié et documenté les ressources sous-exploitées, étudiez l'élimination des jonctions, des ports et des autocommutateurs inutilisés, de manière à réduire les frais de service et/ou de maintenance du réseau.

Affichage du retour sur investissement

Après avoir identifié les modifications de la capacité possibles, vous pouvez calculer et présenter les économies mensuelles possibles à partir des jonctions éliminées et la différence dans les coûts de maintenance entre la configuration actuelle et la future.

Pour évaluer le retour sur investissement :

1. Etudiez vos frais d'utilisation mensuels pour identifier le coût des lignes louées qui risquent d'être sous-exploitées.

2. Etudiez vos frais de maintenance de port pour identifier les coûts des ports inutilisés.

3. Contactez vos fournisseurs de service pour identifier les éventuels coûts de modification de service ou de réduction du nombre de ports. Si vous avez des coûts internes de modification de service, prenez-les en compte.

4. Calculez le retour sur investissement des modifications à l'aide de l'équation suivante :

   Retour sur investissement = (modification de service + frais de modification de port) / économies mensuelles

5. En fonction de vos calculs sur le retour sur investissement, déterminez s'il est pertinent d'effectuer les modifications suggérées.

Traitement et confirmation des ressources surexploitées

L'outil Capacity Analyzer fournit le trafic de pointe d'un délai défini, ainsi que le nombre requis de jonctions ou de ports afin de traiter la charge de trafic pour obtenir la qualité d'écoulement du trafic voulue.

Procédez comme suit pour confirmer les résultats de la surexploitation :

- Réexécutez l'outil Capacity Analyzer et sélectionnez une plage de dates plus précise. Par exemple, si un rapport trimestriel présente des utilisations qui semblent anormalement en dehors des plages des heures de pointe, faites l'évaluation chaque mois afin de visualiser le modèle ou les tendances des données des heures chargées. Cela peut vous aider à déterminer si cette heure chargée constitue une anomalie ou si le trafic s'accroît sur le réseau. Si l'heure de pointe est liée à un événement ponctuel, vous pouvez ignorer cette activité atypique dans votre planification de la capacité.
- L'exécution de rapports de trafic de voix pour la plate-forme montre les tendances de l'utilisation des jonctions ou des ports. Ainsi, vous pouvez voir tout dépassement dans un autre groupe de jonctions.
- Vérifiez la qualité d'écoulement du trafic sélectionnée avec le technicien chargé des autocommutateurs/autocommutateurs IP de ce groupe de jonctions. Confirmez que votre analyse de chaque groupe de jonctions utilise la qualité d'écoulement du trafic initialement destinée ou planifiée pour ce groupe.
- Contactez votre fournisseur de service pour augmenter la capacité, par exemple en ajoutant des jonctions au groupe de recherche ou dans un T1 fractionnel.



Analyse de la capacité de disque de la messagerie vocale

L'outil Capacity Analyzer vous permet de vérifier la capacité de la zone de message dans les services de messagerie vocale. Si l'espace disque est insuffisant, les utilisateurs ne peuvent pas créer de messages vocaux. Dans le cadre des activités qui utilisent la messagerie vocale pour enregistrer des bons de commande ou pour gérer des ressources, les problèmes d'espace disque peuvent engendrer de graves conséquences sur le service.

Pour analyser la capacité de disque de la messagerie vocale :

1. Dans la boîte de dialogue Capacity Analyzer, sélectionnez l'onglet Voice Messaging Disk Analysis.

2. Etudiez la boîte de dialogue pour obtenir des informations sur l'utilisation du disque et les statistiques des jours chargés, afin de déterminer si les serveurs de messagerie vocale sont capables de prendre en charge leur volume habituel et d'identifier les jours les plus chargés.

Résolution des problèmes de capacité de disque

Si vos services de messagerie ont un espace disque insuffisant, procédez comme suit pour résoudre les problèmes de capacité :

- Demandez aux utilisateurs de supprimer les messages anciens/superflus pour libérer de l'espace disque.
- Réfléchissez à la mise en place de restrictions de longueur sur les messages vocaux, de limites temporelles sur la durée d'enregistrement des messages et de limites sur le nombre de messages enregistrés. Ainsi, vous pouvez mieux prévoir l'utilisation de l'espace disque pour les boîtes aux lettres.
- Si les méthodes de conservation ne libèrent pas suffisamment d'espace disque, augmentez la capacité de disque des serveurs de messagerie.



(Page laissée intentionnellement vide)



Chapitre 10 : Résolution rapide des problèmes

Sur un réseau, le moindre problème peut affecter de nombreux services et fonctionnalités. Les systèmes de gestion réseau détectent ces problèmes et peuvent souvent envoyer desflux d'événements pour signaler les ralentissements, les interruptions et les services affectés. Ce torrent d'informations, bien qu'exact, gêne souvent les opérations de dépannage, simplement à cause du volume de données que les opérateurs doivent filtrer.

La solution de gestion des réseaux et de la voix de CA vous aide à centrer vos actions de dépannage sur la source du problème. Le logiciel SPECTRUM effectue une corrélation des événements, une analyse d'impact et une analyse de la cause première pour plusieurs fournisseurs et technologies sur les infrastructures de réseau, système, de voix et d'applications. Il combine les fonctions d'*e*Health dédiées à la recherche et à la génération de rapports sur les modifications de comportement des performances avec les fonctions de surveillance des stratégies et des capacités des réseaux de voix d'*e*Health for Voice. CA offre ainsi une solution clé pour identifier les problèmes, cibler rapidement leur source et fournir une présentation plus détaillée des rapports et des tendances historiques.

Ce chapitre décrit le fonctionnement des processus de résolution des problèmes et d'identification de la cause première de SPECTRUM.

Techniques de résolution des problèmes

SPECTRUM offre trois approches intelligentes, automatisées et intégrées de résolution des problèmes :

- IMT basée sur des modèles
- EMS basé sur des règles
- Technologie de corrélation des conditions (CCT) basée sur des stratégies

Le système SPECTRUM repose essentiellement sur des modèles. Ce genre de système s'adapte aux modifications qui se produisent souvent dans les infrastructures informatiques à la demande en temps réel. Les systèmes basés sur des règles sont flexibles ; en effet, ils permettent aux clients d'ajouter leur intelligence sans recourir à des compétences de programmation. SPECTRUM combine le meilleur des deux approches, en utilisant des modèles pour suivre les modifications tout en exploitant des règles faciles à créer qui fonctionnent parallèlement aux modèles et n'impliquent pas des modifications permanentes. Les systèmes basés sur des stratégies permettent d'associer automatiquement des informations en apparence non liées, afin de déterminer les conditions et l'état des périphériques physiques et des services logiques. Ce moteur de corrélation des conditions se combine au moteur de modélisation et au moteur de règles de SPECTRUM pour fournir un niveau supérieur d'analyse horizontale des services.



Vous pouvez placer presque tous les problèmes d'infrastructure de fourniture de service dans l'une des trois catégories suivantes : disponibilité, performance ou seuil dépassé. Les problèmes d'infrastructure se produisent en cas de rupture d'éléments associés au réseau local/étendu, au serveur, au stockage, à la base de données ou à la sécurité. Les problèmes de performances de l'infrastructure se traduisent souvent par des pannes partielles, au cours desquelles les services sont disponibles mais fonctionnent mal. Du point de vue de l'utilisateur, une infrastructure lente est hors fonction. La dernière catégorie regroupe les conditions de comportement anormal, pendant lesquelles les seuils de performances, d'utilisation ou de capacité sont dépassés, alors que les facteurs de demande/charge passent de manière significative au-dessus/sous les références observées.

SPECTRUM, *e*Health et *e*Health for Voice peuvent détecter ces problèmes sur votre réseau et déclencher une alarme lorsqu'ils se produisent. En envoyant toutes les alarmes à SPECTRUM, vous pouvez identifier les causes des problèmes.

Les analyses basées sur des modèles, des règles ou des stratégies dans SPECTRUM comprennent les relations entre les éléments d'infrastructures informatiques et les processus clients ou métier à prendre en charge. C'est par le biais de cette compréhension des relations que SPECTRUM a pu réduire de 70 % le temps d'arrêt; tout en résolvant 90 % des problèmes de disponibilité ou de performance à partir d'un emplacement central. L'analyse de la cause première de SPECTRUM a pu réduire considérablement le nombre d'alarmes tout en faisant passer le délai moyen de réparation de plusieurs heures à quelques minutes. L'architecture de gestion répartie de SPECTRUM s'est également révélée efficace : elle a permis une analyse de la cause première sur plus de 5 millions de périphériques (plus de 20 millions de ports) dans un environnement unique avec un coeur entièrement maillé et redondant et des couches de distribution réseau. Notre approche intégrée de la gestion des problèmes et des performances a permis aux organisations professionnelles, gouvernementales et aux fournisseurs de service du monde entier de gérer leurs activités vitales par le biais des fonctions intelligentes de niveau de service.

Problèmes complexes et solutions puissantes

La gestion des opérations d'infrastructures informatiques est une tâche à la fois difficile, exigeante en termes de ressources et indispensable. Lorsque l'infrastructure connaît une panne ou un ralentissement, il est nécessaire d'utiliser des outils pour mettre en évidence la cause première, supprimer tous les problèmes symptomatiques, définir des priorités en fonction de l'impact sur l'activité et faciliter le dépannage et la réparation afin d'accélérer la restauration du service.

Pour garantir les performances et la disponibilité de l'infrastructure, la plupart des entreprises utilisent une double approche : des conceptions à haute disponibilité, tolérant les pannes et équilibrant les charges des périphériques d'infrastructure et des chemins de communication et une solution de gestion qui permet d'assurer un bon fonctionnement. En réalité, le job de la solution de gestion est plus complexe à cause des environnements haute disponibilité d'aujourd'hui. La solution de gestion doit comprendre la capacité d'équilibre de charge ; elle doit pouvoir suivre les chemins de sauvegarde principaux et tolérant les pannes et comprendre à quel moment les systèmes redondants sont actifs. Il est aussi important d'investir dans la solution de gestion que dans l'infrastructure proprement dite.



Anticipation des problèmes et prévention

Le logiciel de gestion doit permettre d'anticiper les problèmes ou de les empêcher. Les seuils d'utilisation, de performance et de temps de réponse prêts à l'emploi peuvent servir de système d'avertissement précoce (lorsqu'un problème est sur le point de se produire ou qu'une garantie de niveau de service va être dépassée). Si ces seuils peuvent de toute évidence être ajustés à l'environnement d'un client, il est également important de disposer de seuils prêts à l'emploi, adaptés dès le début à vos références de surveillance.

Avant de procéder au dépannage proprement dit, vous devez isoler le problème. Il ne suffit pas d'être conscient du problème et de collecter des données. Pour isoler précisément le problème, vous devez en déterminer l'emplacement ou la source, ainsi que les endroits qui en sont exempts. Si plusieurs problèmes se produisent en même temps, vous devez être capable de définir leur priorité automatiquement, en fonction des clients, des services ou des infrastructures concernés. Il est bien trop onéreux de compter sur une intervention humaine pour déterminer la cause première des problèmes et de trier un flux interminable de problèmes symptomatiques. Chaque minute consacrée à isoler le problème est une minute perdue pour le résoudre.

Impact sur l'activité

Les meilleures solutions de gestion permettent non seulement d'identifier les problèmes, de les isoler et de supprimer tous les événements symptomatiques, mais aussi d'identifier les composants, les services et les clients affectés. Pour l'activité, il est aussi important de comprendre l'impact que la cause première. En cas d'interruptions ou de détériorations des performances, les services métier et leurs utilisateurs sont affectés. Lorsque cela se produit, les utilisateurs ne peuvent généralement pas exécuter leur job de manière efficace, ce qui se traduit par une réduction de la productivité ou de l'efficacité. Parfois, les services fournis aux clients par l'entreprise sont affectés ; en résultent des pertes sur le chiffre d'affaires, des pénalités sur le contrat de niveau de service et une perte de clients.

Dans le cas de grandes entreprises, plusieurs problèmes peuvent survenir simultanément. En connaissant la cause première, l'organisation peut résoudre de manière efficace les problèmes sans perdre de temps à rechercher des symptômes. La conscience de l'impact permet à l'organisation de définir la priorité des efforts de réponse et de fournir des services d'assistance de qualité.

Corrélation des événements et analyse de la cause première : une approche tridirectionnelle

L'analyse de la cause première de SPECTRUM repose sur les principes suivants :

- Le système doit comprendre la relation entre les informations dans l'infrastructure et les systèmes/applications/services/clients qui en dépendent.
- Le système doit être proactif au niveau de la surveillance et ne pas reposer sur les flux d'événements.
- Le système doit faire la différence entre de nombreux événements et des alarmes significatives.
- Le système doit procéder à une mise à l'échelle et s'adapter aux caractéristiques d'infrastructures en plein développement et dynamiques.
- La solution doit fonctionner avec des produits de divers fournisseurs et technologies.
- Le système doit accepter les extensions et la personnalisation.



Les applications logicielles de gestion qui effectuent correctement l'analyse de la cause première doivent déclencher une alarme pour la condition première et doivent empêcher tout symptôme/effet résultant du fait que la condition première est présentée comme une alarme unique ou distincte.

SPECTRUM dépend de plusieurs techniques combinées pour fournir une corrélation des événements et des fonctionnalités d'analyse de la cause première, notamment IMT, EMS et CCT. Chacune de ces techniques permet de diagnostiquer un ensemble de problèmes variés et souvent imprévisibles.

Analyse de la cause première

L'analyse de la cause première peut être définie comme l'interprétation d'un ensemble de symptômes/événements et la mise en évidence de leur source. Dans le contexte de la gestion d'une infrastructure, les événements sont des occurrences d'actions importantes, présentées à partir d'une source à d'autres systèmes. Les événements appartiennent généralement à une source locale et sans contexte propre, ce qui n'aide pas l'analyse de la cause première.

La corrélation des événements est souvent requise pour déterminer si un problème ou une condition exécutable existe ; elle est presque toujours requise pour isoler les problèmes, identifier tous les composants et les services affectés et supprimer tous les événements symptomatiques. De nombreux composants fournissent des événements sous diverses formes : traps SNMP, messages syslog, entrées de fichier journal d'application, événements TL, flux ASCII, etc. Des systèmes de gestion plus sophistiqués tels que SPECTRUM, *e*Health et *e*Health for Voice peuvent aussi générer des événements en fonction de l'interrogation proactive de l'état des composants, de dépassements de seuils basés sur des paramètres, de dépassements de seuils de mesure du temps de réponse, d'écarts par rapport aux performances historiques et d'analyse de la santé.

L'analyse de la cause première de SPECTRUM est le processus automatique de dépannage de l'infrastructure et d'identification des éléments gérés qui n'ont pas réussi à remplir leur fonction. L'objectif de l'analyse de la cause première de SPECTRUM est d'identifier immédiatement une seule source d'échec, la cause première, et de générer l'alarme exécutable appropriée pour l'élément géré en échec.

Technologie de modélisation inductive

Au coeur de la solution d'analyse de la cause première de SPECTRUM se trouve sa technologie de modélisation inductive (IMT) brevetée. IMT utilise un paradigme de modélisation orienté objet puissant avec des analyses dialectiques basées sur des modèles. Dans SPECTRUM, IMT est la plupart du temps utilisée pour l'analyse topologique physique et logique, car SPECTRUM peut effectuer automatiquement différentes associations topologiques grâce à son moteur de découverte réseau.



Dans SPECTRUM, un modèle est la représentation logicielle d'un élément géré réel ou d'un composant de cet élément géré. Grâce à cette représentation, SPECTRUM peut non seulement rechercher et interroger un élément sur le réseau, mais aussi fournir les moyens pour établir des relations entre des éléments, afin de les reconnaître en tant que parties d'un système plus important. L'analyse de la cause première d'IMT repose sur un système sophistiqué de modèles, de relations et de comportements qui créent une représentation logicielle de l'infrastructure. Les décisions concernant l'élément en rapport avec le problème ne sont pas prises par l'examen d'un seul élément. Au lieu de cela, les relations entre les éléments sont étudiées et les conditions des éléments apparentés sont factorisées dans l'analyse. Les modèles sont en communication directe avec leurs équivalents du monde réel, ce qui permet à SPECTRUM non seulement d'écouter, mais aussi de demander l'état de santé ou des informations de diagnostic supplémentaires. Les modèles sont décrits par leurs attributs, leur comportement, leurs relations avec les autres modèles et leur intelligence algorithmique.

L'analyse intelligente provient de la collaboration de modèles dans un système. Cette collaboration permet la corrélation des symptômes, la suppression des alarmes inutiles et l'analyse d'impact sur les utilisateurs, les clients et les services affectés. Elle inclut la possibilité d'échanger des informations et d'initier le traitement entre tous les modèles du système de modélisation. Un modèle qui envoie une requête à un autre modèle doit à son tour activer ce modèle pour qu'il envoie des requêtes à d'autres modèles et ainsi de suite. Les relations entre les modèles fournissent un contexte de collaboration.

La collaboration entre les modèles déclenche les effets suivants :

- Corrélation des symptômes
- Suppression des alarmes inutiles/symptomatiques
- Analyse d'impact

Pour illustrer l'application d'IMT en action, prenons l'exemple d'un port de routeur réseau passant de l'état UP à DOWN. Si un modèle de port reçoit un trap LINK DOWN, ses fonctions intelligentes lui permettent d'effectuer une requête d'état pour déterminer si le port est réellement arrêté. Si tel est le cas, il consulte le système des modèles pour déterminer si le port possède des sous-interfaces de couches inférieures. Si l'une d'entre elles est également DOWN, seule la condition du port de couche inférieure sera déclenchée comme une alarme. Dans la pratique, cela correspond à plusieurs DLCI de relais de trames passant à l'état INACTIVE. Si le port du relais de trames est arrêté, IMT supprime les conditions DLCI INACTIVE et déclenche une alarme au niveau du modèle de port du relais de trames. De plus, lorsque le port passe à l'état DOWN, IMT demande l'état des éléments réseau connectés ; s'ils sont également DOWN, ces conditions sont considérées comme symptomatiques du port DOWN puis supprimées. Elles sont identifiées comme conséquences de l'alarme du port DOWN. La cause première et l'impact sont déterminés par la faculté d'IMT à écouter l'infrastructure et à communiquer avec elle.



Système Event Management

Parfois, les flux d'événements d'une source spécifique sont la source unique d'informations de gestion. Tout événement unique peut être ou non une occurrence significative ; toutefois, dans l'éventualité d'autres événements, informations ou périodes, il peut s'agir d'une condition exécutable. Les règles d'événements dans le système Event Management de SPECTRUM fournissent un système de prise de décision plus complexe permettant d'indiquer le mode de traitement des événements. Vous pouvez mettre en application les règles d'événements de différentes façons, notamment pour chercher une série d'événements se produisant au niveau d'un modèle dans une certaine structure, dans un délai précis ou avec certaines plages de valeurs de données. Vous pouvez également les utiliser pour générer d'autres événements ou même des alarmes.

Si des événements répondant aux conditions préalables d'une règle se produisent, SPECTRUM doit agir de l'une des façons suivantes :

- Générer un autre événement, ce qui active les événements en cascade
- Consigner l'événement à des fins de génération de rapports ou de dépannage
- Promouvoir l'élément et en faire une alarme exécutable

SPECTRUM fournit six types de règles d'événements personnalisables, qui constituent la base du moteur du système Event Management basé sur des règles.

Ces types de règles forment des blocs qui peuvent être utilisés séparément ou associés, pour générer une alarme sur les scénarios factuels les plus simples ou sophistiqués. Ce moteur de règles du système Event Management permet la corrélation de la fréquence/durée, de la séquence des événements et de leur coïncidence.

Les types de règles d'événements sont les suivants :

- **Event Pair (coïncidence des événements) :** cette règle génère une erreur lorsque le premier des deux événements que vous définissez ne se produit pas dans l'ordre indiqué. Si le deuxième élément d'une série ne se produit pas, il y a peut-être un problème. Le type de règle Event Pair crée un événement plus adapté à ce scénario. Les règles d'événements basées sur le type de règle Event Pair génèrent un nouvel événement lorsqu'un événement se produit sans celui qui lui est associé. Il est possible que d'autres événements se produisent entre la paire d'événements spécifiée sans que cela n'affecte cette règle.
- **Event Rate Counter (fréquence des événements) :** cette règle génère un nouvel événement en fonction des événements qui se produisent à une fréquence précise dans un intervalle de temps spécifié. Quelques événements d'un certain type peuvent être corrects, mais si leur nombre atteint un seuil donné dans une période spécifiée, une notification est requise. SPECTRUM ne génère pas d'autres événements si le taux reste égal ou supérieur au seuil. Si le taux tombe sous le seuil puis repasse au-dessus, un autre événement est généré. Le type Event Rate Counter convient parfaitement à la détection d'une salve longue et constante d'événements.



- **Event Rate Window (fréquence des événements) :** ce type de règle génère un nouvel événement lorsque plusieurs événements identiques sont générés sur une période donnée. Le type Event Rate Window convient parfaitement à la détection précise de salves plus brèves d'événements. Il surveille un événement considéré comme mineur s'il est rare, mais majeur s'il se produit souvent sur une courte période. Un événement peut se produire plusieurs fois dans une journée, sans forcément constituer un problème. Si un événement se produit cinq fois en une minute, il s'agit peut-être d'une condition dont vous souhaitez être averti. Si l'événement se produit au-delà d'un certain taux, SPECTRUM génère un autre événement. SPECTRUM ne génère pas d'autres événements si le taux reste égal ou supérieur au seuil. Si le taux tombe sous le seuil puis repasse au-dessus, un autre événement est généré.
- **Event Sequence (séquence des événements) :** ce type de règle génère un événement lorsque l'ordre d'une séquence d'événements est important dans votre environnement. Cette séquence peut inclure n'importe quel nombre ou type d'événements. Lorsque la séquence est détectée sur la période donnée, SPECTRUM génère un nouvel événement.
- **Event Combo (coïncidence des événements) :** ce type de règle génère un nouvel événement lorsqu'une certaine combinaison se produit dans un ordre quelconque. Elle peut inclure n'importe quel nombre ou type d'événements. Lorsqu'elle est détectée sur une période donnée, SPECTRUM génère un nouvel événement.
- **Event Condition (coïncidence des événements) :** ce type de règle génère un événement en fonction d'une expression conditionnelle. La méthodologie de SPECTRUM repose en partie sur le principe du « Trust but verify » (faire confiance mais vérifier). Il s'agit d'une série d'expressions conditionnelles qui peut être répertoriée dans la règle d'événements. La première expression se révélant TRUE génère l'événement spécifié avec la condition. Vous pouvez établir des règles pour fournir une corrélation par le biais d'une combinaison de données d'événements d'évaluation avec des données de modèle IMT (y compris les attributs lisibles directement depuis l'élément géré distant). Par exemple, si un trap avertissant le système de gestion d'une surcharge du tampon mémoire est reçu, afin de valider qu'une condition d'alarme s'est produite, une règle de condition d'événement peut initier une requête auprès du périphérique afin de verifier l'utilisation réelle de la mémoire.

SPECTRUM implémente un certain nombre de règles d'événements prêtes à l'emploi en appliquant un ou plusieurs types de règles d'événements aux flux d'événements. Vous pouvez créer ou personnaliser des règles d'événements à l'aide de l'un des types de règles et les appliquer à d'autres flux d'événements. Vous trouverez de plus amples informations sur l'implémentation des règles d'événements à l'aide du système Event Management plus loin dans ce document.



Corrélation de conditions

Pour effectuer des corrélations plus complexes définies ou contrôlées par l'utilisateur, SPECTRUM offre une CCT basée sur des règles permettant les fonctions suivantes :

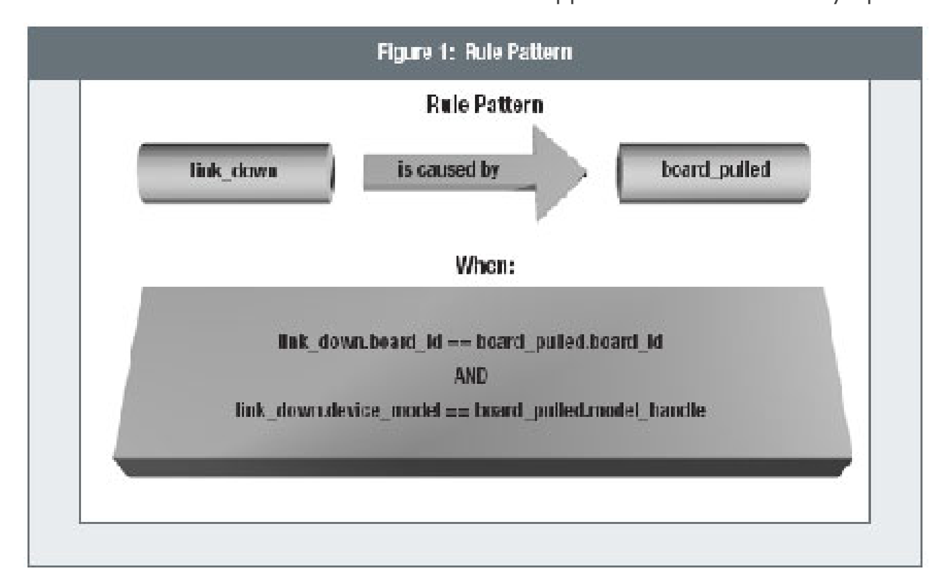
- Création de règles de corrélation
- Création de domaines de corrélation
- Corrélation de flux d'événements ou de conditions apparemment disparates
- Corrélation entre des ensembles d'éléments gérés
- Corrélation dans des domaines gérés
- Corrélation entre des ensembles de domaines gérés
- Corrélation de conditions de composants, avec lien vers des concepts d'ordres supérieurs tels que les services métier ou l'accès client

Plusieurs concepts importants sont liés à la corrélation des conditions :

- **Conditions :** une condition est similaire à l'état. Un événement/une action peut définir une condition et la supprimer. Un événement peut également définir une condition, mais la suppression de la condition nécessite l'intervention d'un utilisateur. Une condition existe dès qu'elle est créée et jusqu'à sa suppression. Un port arrêté est un exemple très simple de condition. La condition Port DOWN existe pour une interface donnée dès que le trap LINK DOWN ou l'événement défini (tel qu'une interrogation d'état en échec) jusqu'à ce que le trap LINK UP ou l'événement supprimé (tel qu'une interrogation d'état de réussite) soit reçu. Dans SPECTRUM, un certain nombre de conditions utiles pour l'établissement de corrélations de niveaux de domaines sont définies et prêtes à l'emploi. Vous pouvez également en ajouter.
- **Conditions apparemment disparates :** de nombreux périphériques d'une infrastructure informatique offrent une fonction spéciale. La fonction de niveau de périphérique n'a souvent pas de contexte car elle est apparentée aux fonctions des autres périphériques/composants. La plupart des éléments gérés peuvent émettre des flux d'événements, mais ces derniers restent spécifiques à chaque composant. Par exemple, lorsque le système de gestion du temps de réponse identifie une condition d'un résultat de test dépassant un seuil. En même temps, un système de gestion des éléments peut identifier la condition d'un port de routeur dépassant un seuil de bande passante de transmission. Ces conditions sont en apparence disparates, car elles sont créées indépendamment et sans contexte ou connaissance des autres. En réalité, les deux sont souvent étroitement liées ; c.-à-d. qu'un port surexploité peut être responsable d'une détérioration des réponses.



- **Modèles de règles :** ils associent des conditions lorsque certains critères sont remplis. Par exemple, l'arrêt d'un port peut être dû à une carte extraite. Les deux conditions sont probablement liées si le port et la carte ont le même numéro d'emplacement. Le graphique suivant montre le modèle de règle. Un modèle de règle peut engendrer la création d'une alarme exécutable ou la suppression des alarmes symptomatiques.



- **Domaines de corrélation :** vous pouvez utiliser un domaine de corrélation à la fois pour définir et limiter la portée d'une ou de plusieurs stratégies de corrélation. Vous pouvez l'appliquer à un service spécifique. Par exemple, dans l'environnement de câblage à large bande, un système de surveillance du chemin de retour peut détecter un échec du chemin de retour dans une zone de service précise. Du fait de cette condition d'échec du chemin de retour, les modems câblés haute vitesse de l'abonné deviennent inaccessibles et ses flux de vidéo à la demande avec paiement à la carte échouent. Pour corréler les événements et identifier la cause première, il est essentiel de savoir que l'échec du chemin de retour, les problèmes de modem et l'échec des flux vidéo se trouvent tous dans le même domaine de corrélation. Toutefois, il est également important de savoir qu'une condition d'échec du chemin de retour se produisant dans un domaine de corrélation (Philadelphie) ne doit pas être corrélée à des conditions d'échec de flux de vidéo à la demande se produisant dans un domaine de corrélation différent (New York).
- **Stratégies de corrélation :** vous pouvez regrouper plusieurs modèles de règles dans des stratégies de corrélation. Vous pouvez ensuite appliquer ces dernières à un service ou à un domaine de corrélation. Par exemple, vous pouvez créer un ensemble de modèles de règles applicables au protocole OSPF et les intituler OSPF Correlation Policy. Vous pouvez appliquer la stratégie OSPF Correlation Policy à chaque domaine de corrélation, où chaque zone OSPF est autonome et où les routeurs de base de cette zone définissent le domaine de corrélation. Par exemple, vous pouvez définir la stratégie de corrélation en fonction d'un jeu de modèles de règles fonctionnant dans les limites d'un VPN MPLS/BGP intitulé Intra-VPN Policy et l'appliquer à tous les VPN modélisés. Dès que vous ajoutez une règle à une stratégie de corrélation ou que vous en supprimez une, SPECTRUM met automatiquement et immédiatement à jour tous les domaines de corrélation. Vous pouvez appliquer plusieurs stratégies de corrélation à un domaine de corrélation et appliquer une stratégie de corrélation à plusieurs domaines de corrélation.



Les corrélations basées sur des conditions sont très puissantes et fournissent un mécanisme permettant de développer des stratégies de corrélation et de les appliquer à des domaines de corrélation. Lorsque vous les appliquez à la gestion des niveaux de services, les stratégies de corrélation sont similaires aux mesures d'un contrat de niveau de service et les domaines de corrélation sont similaires aux regroupements de services, de clients ou géographiques. Parfois, vous pouvez déduire une relation de cause à effet entre plusieurs conditions apparemment disparates uniquement si ces dernières se produisent dans un domaine de corrélation commun. Ces mécanismes sont nécessaires lorsque les interrogations ne permettent pas à SPECTRUM de trouver les relations de cause à effet.

Scénarios de défaillance

Prêt à l'emploi, SPECTRUM traite divers scénarios sur lesquels il peut effectuer une analyse de la cause première. Cette section fournit des scénarios spécifiques dans lesquels les techniques décrites dans la section précédente déterminent l'analyse de la cause première et de l'impact Par souci de simplicité et de concision, les détails se limitent au traitement de base. De plus, pour faciliter la discussion et la visibilité des chiffres, le tableau suivant montre la couleur des alarmes associées à l'état d'icône des modèles SPECTRUM à un moment donné.

Etat du modèle	Couleur d'alarme
Fonctionnement normal	VERT
Erreur critique	ROUGE
Erreur grave	ORANGE
Erreur mineure	JAUNE
Inconnu ou supprimé	GRIS
Arrêté pour maintenance	MARRON
Etat initial	BLEU

Interruptions de communication et répercussions

Les interruptions de communication sont des problèmes souvent décrits comme des coupures ou des erreurs matérielles. Avec ces types de problèmes, les chemins de communication sont détériorés à un tel point que le trafic ne peut plus passer. Le problème peut être dû à de nombreuses situations : des câbles/connexions en cuivre/fibres rompus, des routeurs/commutateurs mal configurés, des pannes matérielles, de graves problèmes de performances, des attaques de sécurité, etc. Du fait de ces problèmes de communication, les informations qui sont disponibles pour le système de gestion sont limitées car il est impossible d'échanger des informations avec un ou plusieurs éléments gérés. Avec son système sophistiqué de modèles, de relations et de comportements disponibles via IMT, SPECTRUM peut déduire le problème et l'impact. Les algorithmes d'interprétation d'IMT sont également appelés Gestionnaires d'interprétation. Pour désigner un ensemble de gestionnaires d'interprétation prévu pour un objectif précis, on utilise le terme Circuit d'interprétation ou tout simplement Intelligence.



Isolation des interruptions de communication grâce à l'intelligence de SPECTRUM

SPECTRUM offre de puissantes fonctionnalités permettant d'identifier les véritables sources des problèmes du réseau. Dans de nombreuses solutions de gestion, les étapes permettant d'exécuter cette fonctionnalité sont souvent manuelles et demandent beaucoup de temps. Toutefois le logiciel SPECTRUM effectue automatiquement bon nombre de ces étapes.

SPECTRUM identifie et isole les interruptions de la manière suivante :

1. Utilisez la fonction de découverte de SPECTRUM pour créer un modèle de votre infrastructure qui indique les ressources de votre réseau et la façon dont elles sont connectées.
2. Lorsqu'il reçoit un événement problématique, SPECTRUM vérifie l'état de ressources étroitement connectées pour déterminer si elles présentent des problèmes.
3. SPECTRUM analyse l'état des ressources pour identifier la cause première probable du problème.
4. SPECTRUM supprime les alarmes symptomatiques de la cause première, mais pas la cause proprement dite.
5. SPECTRUM évalue la gravité du problème afin d'en déterminer la priorité par rapport aux autres problèmes signalés dans le réseau.

Les sections suivantes décrivent les fonctionnalités de SPECTRUM de manière plus détaillée.

CRÉATION DU MODÈLE À L'AIDE DE LA FONCTION AUTODISCOVERY

Une représentation précise de l'infrastructure est vitale pour déterminer la défaillance et l'impact associé. Le système de modélisation de SPECTRUM représente non seulement un large éventail d'équipements multifournisseurs, mais également une gamme étendue de technologies et de connexions pouvant exister entre divers éléments d'infrastructure. SPECTRUM comporte des solutions spécifiques de découverte de réseaux multiplates-formes via une variété de technologies qui prennent en charge différentes architectures. SPECTRUM prend en charge les topologies maillées et redondantes, physiques et logiques basées sur des environnements ATM, Ethernet, Frame Relay, HSRP, ISDN, ISL, MPLS, Multicast, PPP, VoIP, VPN, VLAN et 802.11 sans fil, y compris des technologies traditionnelles telles que FDDI et Token Ring. La modélisation de SPECTRUM est très extensible et peut s'appliquer aux couches OSI 1à 7 dans une infrastructure de communication.



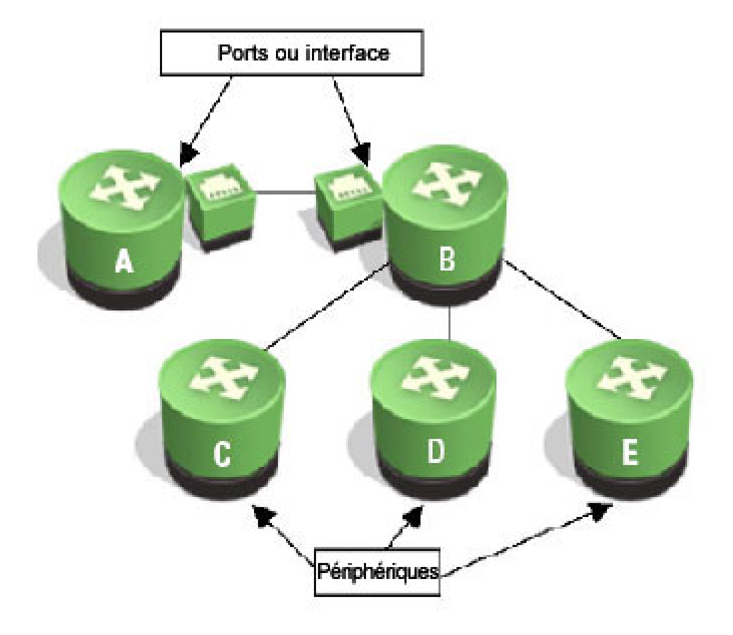
SPECTRUM propose quatre méthodes de création d'un modèle de connectivité de topologie physique et logique pour une infrastructure spécifique :

- L'application SPECTRUM AutoDiscovery interroge de façon automatique et dynamique l'infrastructure gérée pour connaître ses relations physiques et logiques. Parmi tous les produits du secteur, SPECTRUM a été le premier à découvrir la couche 2 de la connectivité des commutateurs. L'application SPECTRUM AutoDiscovery s'exécute en deux phases distinctes (bien que chacune de ces phases comporte de nombreuses étapes non décrites ici). La première phase est la découverte. Une fois lancée (voir chapitre 5), l'application AutoDiscovery découvre automatiquement les éléments présents dans l'infrastructure. SPECTRUM contient alors un inventaire des éléments qui peuvent être gérés. La seconde phase est la modélisation. AutoDiscovery utilise les protocoles de gestion et de découverte pour interroger les éléments trouvés afin d'obtenir des informations qui serviront à déterminer les couches 2 et 3 de connectivité entre les éléments gérés. Par exemple, AutoDiscovery utilise le protocole SNMP pour examiner les tables de routage, de passerelle et d'interface. L'application utilise également des protocoles d'analyse du trafic et de découverte propriétaire des fournisseurs tels que Cisco CDP. AutoDiscovery est un mécanisme automatique exhaustif de création du modèle d'infrastructure.
- La passerelle de modélisation importe une description de tous les composants de l'infrastructure, ainsi que les informations sur la connectivité physique et logique provenant de sources externes, par exemple des systèmes d'approvisionnement ou des bases de données de topologie réseau.
- L'interface de ligne de commande ou les API de programmation peuvent créer une intégration ou une application personnalisée dans laquelle importer les informations des sources externes.
- Les interfaces utilisateur graphiques permettent aux utilisateurs de pointer facilement sur des éléments, puis de cliquer dessus et de les faire glisser pour créer manuellement le modèle.

Le plan de modélisation de SPECTRUM permet de décomposer un élément géré unique en un nombre quelconque de sous-modèles. Cet ensemble de modèles et les relations associées est souvent désigné comme un modèle de données sémantique pour ce type d'élément géré. Ainsi, le modèle de données sémantique d'un périphérique en réseau peut inclure un modèle de châssis lui-même lié à des modèles de cartes. Des modèles d'interface physique sont associés aux modèles de cartes. Un ensemble de modèles de sous-interfaces est associé à chaque modèle d'interface physique.

SPECTRUM comporte un ensemble d'associations précises qui définissent les différences de comportement des modèles de données sémantiques les uns par rapport aux autres. Lorsque SPECTRUM représente la connectivité entre deux périphériques, une relation est établie non seulement entre les deux ports qui forment cette liaison, mais également entre les modèles de périphériques et vers les modèles d'interfaces et de ports correspondants des autres périphériques, comme indiqué dans la figure ci-dessous.

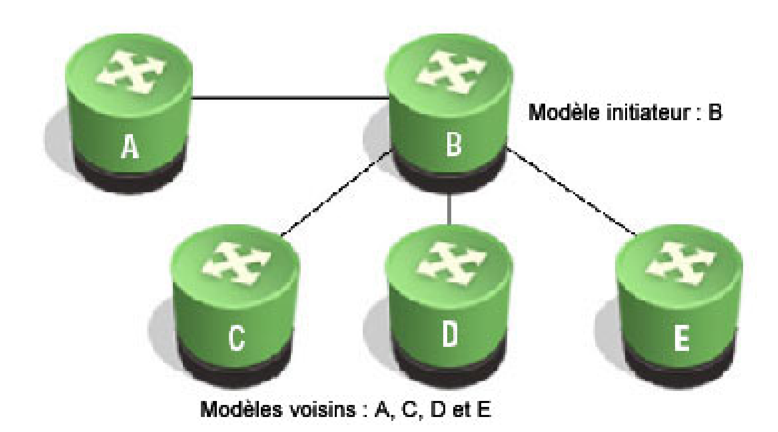




DÉBUT DE L'ANALYSE DU PROBLÈME

SPECTRUM peut commencer à résoudre un problème de manière proactive dès qu'un symptôme est détecté. Plusieurs problèmes pouvant présenter les mêmes symptômes, SPECTRUM doit effectuer une analyse plus approfondie afin de déterminer la cause première. Lors d'interruptions de communication, l'analyse démarre lorsqu'un modèle de SPECTRUM identifie les erreurs de communication suivantes : échecs d'interrogations, de traps et d'événements, dépassements de seuils de performances ou absence de réponse. SPECTRUM valide automatiquement les erreurs de communication en vérifiant les relances, ainsi que les protocoles et les chemins alternatifs, conformément à la méthodologie « Trust but verify ». Le modèle qui a détecté le problème et lancé la fonction intelligente est appelé l'initiateur, bien que plusieurs modèles puissent déclencher cette fonction.

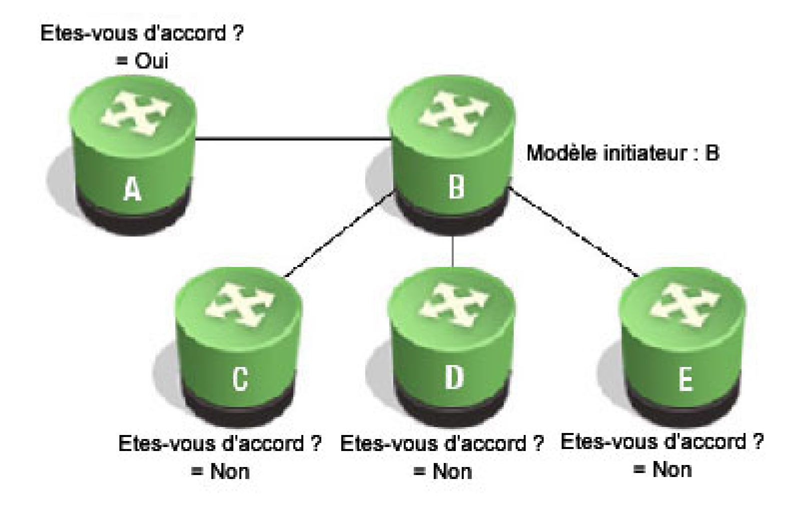
Le modèle initiateur demande une liste des autres modèles auxquels il est directement connecté. Ces modèles connectés sont désignés comme les voisins du modèle initiateur. Par exemple, la figure suivante présente cinq modèles : le modèle B est l'initiateur, les modèles A, C, D et E sont les voisins.





Une fois la liste des voisins identifiée, la fonction intelligente demande à chaque modèle voisin de vérifier son état actuel. Cette vérification s'effectue par le biais d'une question : Etes-vous OK ? OK est un terme relatif ; il désigne un ensemble unique d'attributs associés aux performances et à la disponibilité qui varie d'un modèle à l'autre en fonction des capacités réelles du périphérique représenté par le modèle.

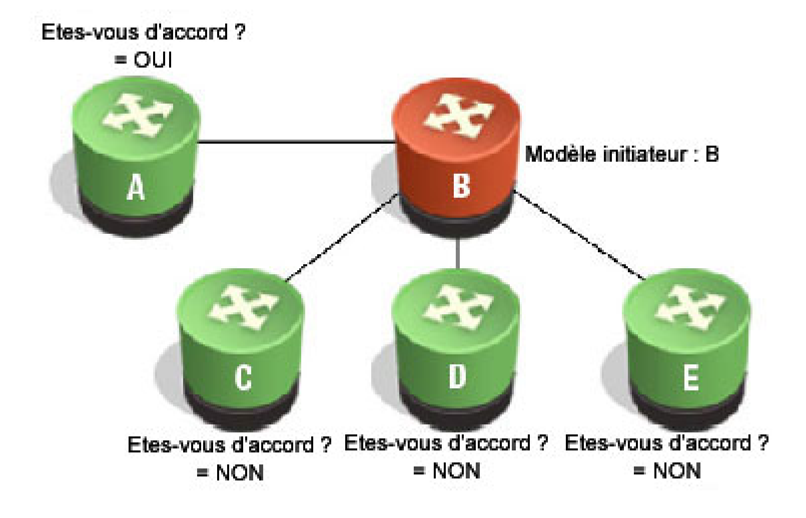
Lorsqu'un modèle doit répondre à la question « Etes-vous OK ? », il peut lancer divers tests/contrôles afin de vérifier son état de fonctionnement actuel. Par exemple, avec la plupart des éléments gérés via SNMP, cette vérification constitue généralement une combinaison de requêtes SNMP, mais elle peut également inclure l'interrogation d'un système de gestion d'éléments ou prendre la forme d'une simple requête ping ICMP. Une vérification complète comprend le calcul des seuils de performances ou l'exécution de tests de temps de réponse.



Chaque modèle voisin répond à la question Etes-vous OK ?.

RECHERCHE DE LA CAUSE PREMIERE, ISOLATION DES DEFAILLANCES

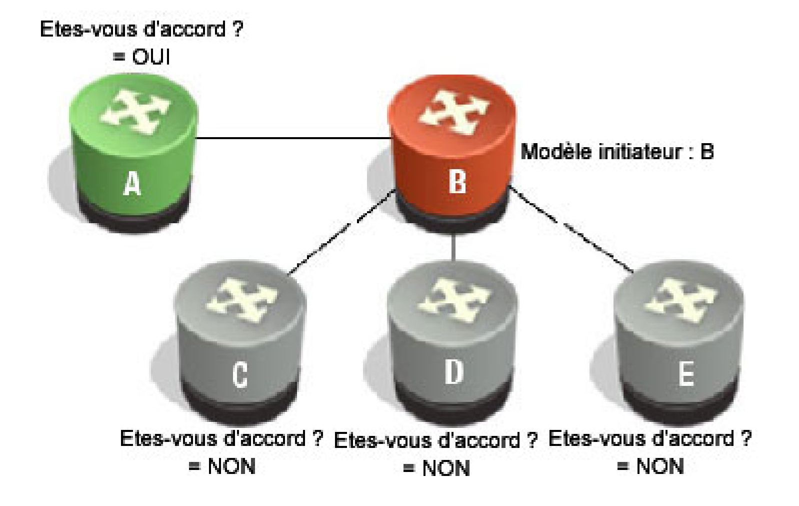
Si un voisin du modèle initiateur répond Oui à cette question, par exemple le modèle A de la figure précédente, SPECTRUM peut en déduire que le problème réside entre le voisin non affecté et l'initiateur affecté (modèle B). Dans ce cas, il est possible que le modèle initiateur qui a déclenché la fonction intelligente soit à l'origine de cette erreur d'infrastructure. Par conséquent, SPECTRUM déclenche une alarme critique de cause première sur le modèle initiateur, comme indiqué dans la figure suivante.





ELIMINATION DES INTERFÉRENCES LIÉES AUX PROBLÈMES SYMPTOMATIQUES PAR LA SUPPRESSION DE L'ALARME

Une fois le périphérique défectueux isolé (modèle B), l'étape suivante consiste à analyser et supprimer les rapports sur les effets de la défaillance. C'est le but de la suppression d'alarme intelligente. Si un voisin (tel que le modèle C, D ou E) du modèle initiateur répond qu'il n'est pas OK, il est considéré comme affecté par la défaillance présente ailleurs dans l'infrastructure. Par conséquent, SPECTRUM place ces modèles dans la condition supprimée (couleur grise) car les alarmes sont symptomatiques d'un problème survenu ailleurs. Bien que ces ressources soient défaillantes, elles ne constituent pas la cause première ; elles seront donc résolues après les problèmes affectant le modèle B.



PRIORITÉ DU PROBLÈME : ANALYSE D'IMPACT

SPECTRUM poursuit l'analyse de l'impact total de la défaillance grâce à sa capacité à comprendre que chaque modèle appartient à un réseau plus étendu de modèles représentant l'infrastructure gérée.

Ainsi, sa fonction intelligente analyse chaque domaine de défaillance, qui est l'ensemble des modèles ayant eu des alarmes supprimées liées à la même erreur. Ces modèles affectés sont liés à la défaillance racine en termes de présentation et d'analyse. La fonction intelligente mesure l'impact de cette défaillance en examinant les modèles inclus dans le domaine de défaillance et en calculant une mesure qui indique la gravité de l'impact. La valeur de gravité de l'impact fournit un système de classement qui permet aux opérateurs de rapidement évaluer l'impact relatif de chaque défaillance d'infrastructure afin de définir la priorité des actions correctives.



Système Event Management

Les règles d'événements approfondissent le traitement et la corrélation des flux d'événements. Le traitement des règles d'événements est requis lorsque le flux d'événements est la seule source des informations de gestion. Par exemple, SPECTRUM Southbound Gateway permet à SPECTRUM d'accepter les flux d'événements provenant de périphériques et d'applications qu'il ne surveille pas directement, par exemple les autocommutateurs privés *e*Health for Voice et les serveurs de messagerie. Vous pouvez également appliquer des règles d'événements pour effectuer un traitement intelligent des événements dans certains contextes (fréquence, séquence, combinaison). Comme décrit plus haut dans ce chapitre, vous pouvez appliquer six types de règles d'événements :

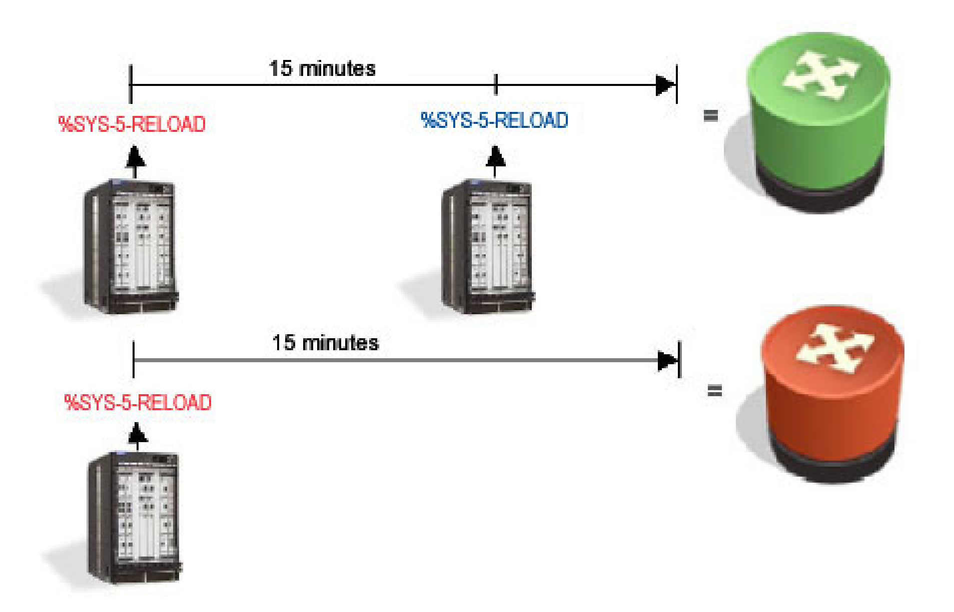
- Event Pair : événement de paire attendu ou manquant dans un intervalle de temps spécifique.
- Event Rate Counter : événements qui se produisent à une fréquence précise dans un intervalle de temps spécifique.
- Event Rate Window : nombre d'événements dans un intervalle de temps spécifique.
- Event Sequence : séquence ordonnée d'événements dans un intervalle de temps spécifique.
- Event Combo : combinaison de plusieurs événements dans un ordre quelconque et dans un intervalle de temps spécifique.
- Event Condition : événements analysés à la recherche de données spécifiques pour créer des événements à partir de la comparaison de liaisons de variables, d'attributs, de constantes, etc.

SPECTRUM fournit de nombreuses règles d'événements prêtes à l'emploi, ainsi que des méthodes simples de création de règles à l'aide d'un ou plusieurs types de règles d'événements. Cette section présente quelques règles d'événements prêtes à l'emploi et des exemples d'applications pour les clients.

REGLE EVENT PAIR PRETE A L'EMPLOI

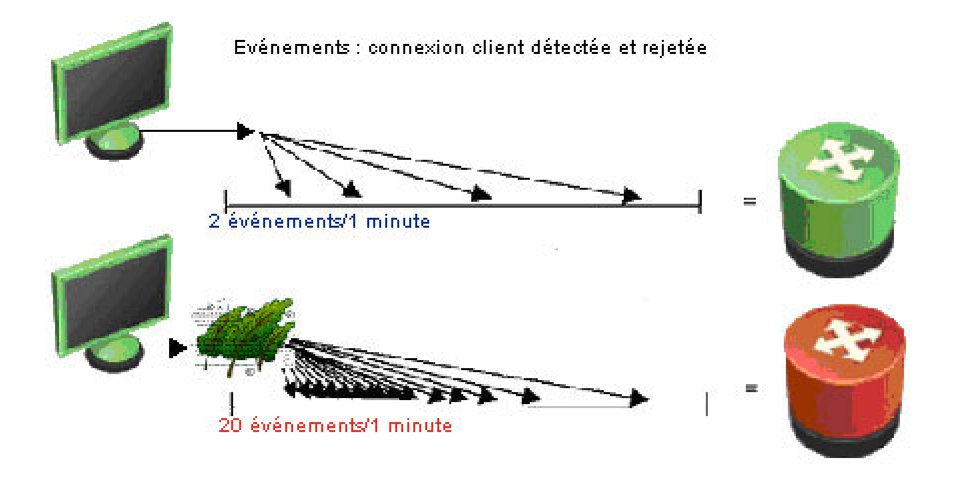
SPECTRUM permet d'interpréter les messages syslog Cisco comme des flux d'événements. Chaque message syslog est généré au nom d'un commutateur ou routeur géré et transmis au modèle SPECTRUM représentant cet élément géré. L'un des nombreux messages syslog Cisco indique le chargement d'une nouvelle configuration dans le routeur. Le message Reload doit toujours être suivi d'un message Restart indiquant le redémarrage du périphérique pour adopter la configuration chargée. Sinon, une erreur risque de se produire lors du rechargement. SPECTRUM utilise une règle d'événement basée sur le type de règle Event Pair qui déclenche l'alarme ERROR DURING ROUTER RELOAD si le message Restart n'apparaît pas dans un délai de 15 minutes suivant le message Reload. Le graphique ci-dessous illustre les événements et le minutage.





GESTION DES ÉVÉNEMENTS DE SÉCURITÉ À L'AIDE D'UNE RÈGLE EVENT RATE COUNTER

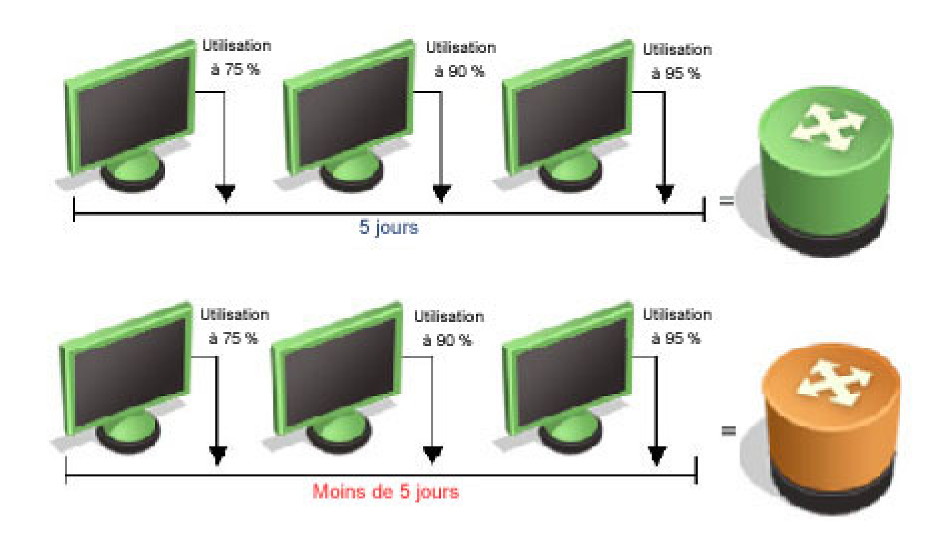
SPECTRUM permet de collecter les flux d'événements à partir de diverses sources. Certains clients envoient des événements à partir de dispositifs de sécurité tels que des systèmes de détection d'intrusion et des pare-feux. Ces types de dispositifs peuvent générer des millions d'entrées de fichier journal. Les clients peuvent utiliser une règle Event Rate Counter pour distinguer les rejets sporadiques de connexion client des véritables attaques de sécurité. La règle génère une alarme critique si 20 échecs de connexion ou plus se sont produits en moins d'une minute, comme indiqué dans la figure suivante.





GESTION DE LA CROISSANCE DE LA MÉMOIRE DU SERVEUR À L'AIDE D'UNE RÈGLE EVENT SEQUENCE

Dans certaines applications, il est souvent impossible de gérer l'utilisation de la mémoire. Elles utilisent une mémoire système qui ne peut jamais être ensuite allouée à d'autres applications. Cela peut dégrader les performances de l'ordinateur hôte, voire entraîner l'échec de l'application qui perd de la mémoire. A titre d'exemple, si vous possédez une application de serveur Web qui a déjà rencontré quelques problèmes de fuite de mémoire, vous pouvez planifier un redémarrage hebdomadaire dans le cadre des opérations de maintenance prévues afin de compenser la consommation de mémoire. Toutefois, si la fuite de mémoire s'accélère, créant un comportement anormal, vous pouvez effectuer un redémarrage d'urgence avant la maintenance planifiée. Vous pouvez combiner des seuils SPECTRUM progressifs avec une règle Event Sequence pour surveiller le comportement anormal ou utiliser la fonction d'analyse *e*Health Live Health pour signaler l'écart par rapport à la consommation de mémoire normale. En utilisant les seuils SPECTRUM comme exemple, vous pouvez configurer la surveillance de manière à créer des événements lorsque l'utilisation de la mémoire franchit les points de seuil de 50 %, 75 % et 90 %. Si ces points de seuil sont atteints en moins d'une semaine, SPECTRUM génère une alarme indiquant la nécessité de redémarrer le serveur avant l'opération de maintenance planifiée, comme indiqué dans le schéma suivant.



RÈGLE EVENT CONDITION PRÊTE À L'EMPLOI COMBINÉE À UNE RÈGLE EVENT PAIR

RFC2668 (MIB pour unités de connexion au support IEEE 802.3) fournit des définitions de gestion pour les concentrateurs Ethernet. Cette RFC contient la définition d'un trap SNMP servant à avertir un système de gestion lorsque l'état de brouillage d'une interface change. Le brouillage survient lorsqu'un périphérique qui rencontre une erreur logique ou de circuit envoie en continu des données aléatoires (incorrectes). L'identificateur de traps indique simplement un changement de condition tandis que la partie contenant les données variables du trap précise si le brouillage a commencé ou s'est arrêté. SPECTRUM applique une règle Event Condition pour créer des événements de démarrage/d'arrêt distincts en consultant la partie variable du trap et utilise une règle Event Pair pour générer une alarme si le début du brouillage n'est pas rapidement suivi d'un événement d'arrêt.

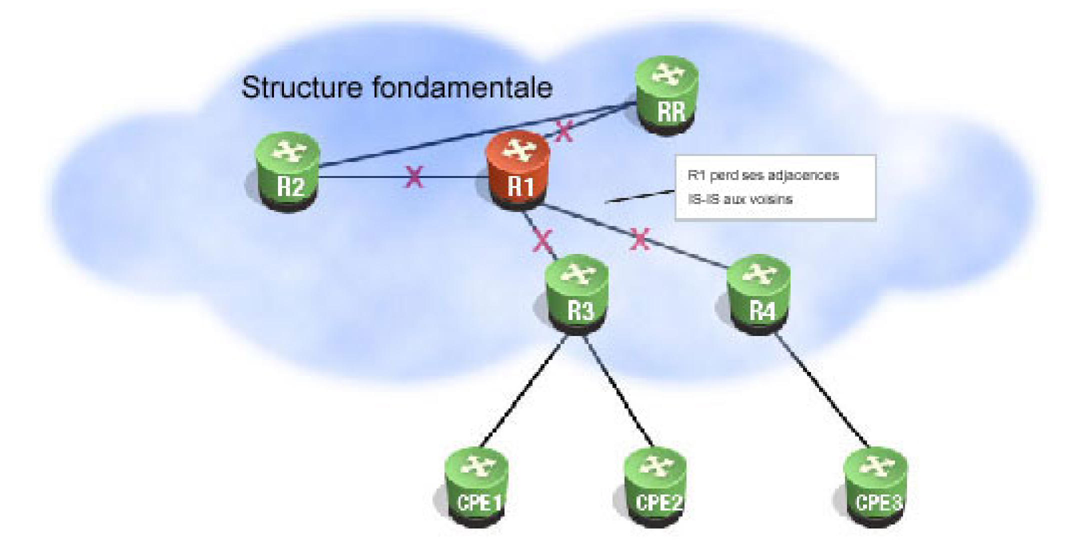


TECHNOLOGIE DE CORRÉLATION DES CONDITIONS

La technologie de corrélation des conditions (CCT) de CA SPECTRUM offre des fonctionnalités avancées de personnalisation qui permettent de définir des relations entreles événements de manière à isoler les causes premières des problèmes. Par exemple, étudiez les complexités liées à la gestion d'un réseau IP assurant la connectivité VPN sur une structure fondamentale MPLS avec un routage intrazone effectué via le protocole IS-IS (Intermediate System-to-Intermediate System) et un routage interzone réalisé via BGP. Tout échec de protocole ou de liaison physique peut déclencher des dizaines d'événements à partir d'une multitude de périphériques. S'ils n'appliquent pas la corrélation sophistiquée avec soin, les dépanneurs réseau peuvent perdre un temps considérable à rechercher des symptômes au lieu de résoudre la cause première.

EXEMPLE D'ÉCHEC DE ROUTAGE IS-IS

L'exemple suivant illustre l'étendue des fonctionnalités de la corrélation des conditions. Un routeur principal, nommé R1 dans la figure, a perdu sa contiguïté IS-IS avec tous ses voisins (intitulés R2, R3 et R4). Cela entraîne la perte de la session BGP avec le réflecteur de route (nommé RR dans la figure). Si cette situation persiste, R1 et les routeurs de périphérie adjacents R3 et R4 considèrent ces routes comme anciennes. Enfin, les sites VPN clients mis en service par ces routeurs de périphérie ne parviennent pas à accéder à leurs sites homologues (nommés CPE1, CPE2 et CPE3 dans la figure).





Par conséquent, les routeurs génèrent une série de messages d'erreur syslog et de traps. Le tableau suivant présente les messages et les traps reçus par SPECTRUM :

Source	Type	Message
R1	Syslog message	%CLNS-5-ADJCHANGE: ISIS: Adjacency to R2 (POS5/0/0) Down, hold time expired
R1	Syslog message	%CLNS-5-ADJCHANGE: ISIS: Adjacency to R3 (POS5/0/0) Down, hold time expired
R1	Syslog message	%CLNS-5-ADJCHANGE: ISIS: Adjacency to Rn (POS5/0/0) Down, hold time expired
RR	Syslog message	%BGP-5-ADJCHANGE: neighbor R1 Down BGP Notification sent
RR	Syslog message	%BGP-3-NOTIFICATION: sent to neighbor R1 4/0 (hold time expired) 0 bytes
RR	Trap	BGP Backwards Transition trap, neighbor = R1
R2	Syslog message	%CLNS-5-ADJCHANGE: ISIS: Adjacency to R1 (POS5/0/0) Down, hold time expired
R3	Syslog message	%CLNS-5-ADJCHANGE: ISIS: Adjacency to R1 (POS5/0/0) Down, hold time expired
Rn	Syslog message	%CLNS-5-ADJCHANGE: ISIS: Adjacency to R1 (POS5/0/0) Down, hold time expired

Le cause première de tous ces messages est le problème de routage IS-IS lié à R1. Dans la plupart des systèmes de gestion, chacun de ces messages et traps apparaît à l'opérateur ou au dépanneur sous la forme d'un événement apparemment disparate dans la console d'événements/alarmes. Un opérateur qualifié ou un dépanneur expérimenté peut être capable, après une intense réflexion, d'en déduire qu'un problème de routage s'est produit sur R1. Toutefois, dans un environnement de grande taille, ces événements/alarmes sont probablement partagés avec d'autres événements/alarmes encombrant la console. Même si l'opérateur ou le dépanneur a l'habitude d'identifier manuellement la corrélation, cette tâche demande du temps et des efforts. Ce temps est directement lié aux coûts, à la baisse de la satisfaction utilisateur et à la perte de revenus.

Sans corrélation des conditions, SPECTRUM notifierait une dizaine d'événements aux utilisateurs de la console d'alarmes. Toutefois, si vous combinez une règle d'événements et la corrélation des conditions, vous pouvez appliquer un ensemble de modèles de règles à un domaine de corrélation composé de tous les routeurs principaux (LSR), ce qui permet à SPECTRUM de produire une alarme exécutable unique. Cette alarme indique que R1 présente un problème de routage IS-IS, ce qui peut entraîner une interruption de réseau si ce problème n'est pas résolu. Les conditions apparemment disparates corrélées par SPECTRUM déterminent les résultats de l'alarme qui apparaissent dans le volet Symptômes de la console d'alarmes, comme suit :

1. Une règle Event Rate Counter locale a servi à définir plusieurs messages syslog de changement de contiguïté IS-IS renvoyé par la même source que le problème de routage.

2. Un modèle de règle a servi à créer un événement de perte de contiguïté IS-IS causé par un problème de routage IS-IS lorsque le voisin de l'événement de perte de contiguïté correspond à la source de l'événement du problème de routage.

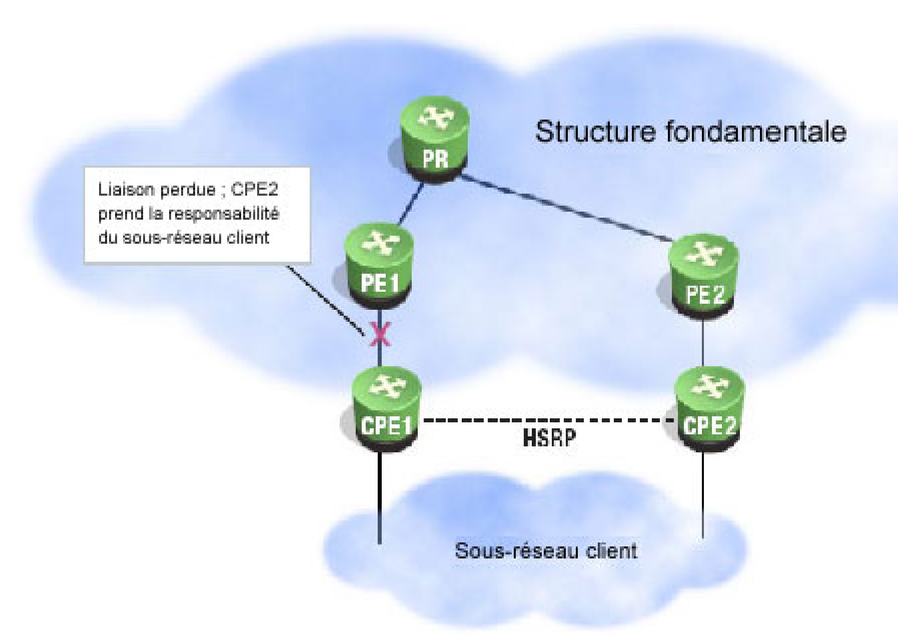
3. Un modèle de règle a servi à créer un événement d'arrêt de contiguïté BGP causé par un problème de routage IS-IS lorsque le voisin de l'événement d'arrêt de contiguïté correspond à la source de l'événement du problème de routage.

4. Un modèle de règle a servi à créer un événement de trap de transition arrière BGP causé par un problème de routage IS-IS lorsque le voisin de l'événement de transition arrière correspond à la source de l'événement du problème de routage.



EXEMPLE D'ÉCHEC DE ROUTAGE HSRP/VRRP

La corrélation des conditions fournit également une corrélation des événements utile et intéressante lors de la perte d'une liaison vers un routeur dans un environnement HSRP (Hot Standby Routing Protocol) ou VRRP (Virtual Router Redundancy Protocol). Dans l'exemple suivant, un site comporte deux routeurs redondants qui fournissent un accès via HSRP. Dans ce cas, le routeur principal rencontre une erreur, mais le routeur redondant continue à servir le site du client. Vous pouvez définir une notification d'alarme pour le basculement redondant et distinguer ce dernier d'une interruption totale du site. L'utilisation des technologies IMT, EMS et CCT peut faciliter l'analyse de la cause première.



Le tableau suivant présente les messages d'erreur syslog et les séquences de traps lors du basculement HSRP.

Source	Type	Message
PE1	Message syslog	%LINK-3-UPDOWN: Interface Serial0/1 changed start to down
PE1	Trap	Link down trap, ifIndex=5, ifOperStatus=Down
PE2	Trap	HSRPGrpStandByState, state=Active
NMS	Echec de l'interrogation	Device Contact Status Lost, Model=CPE1

Le volet Symptômes de la console d'alarmes contient les conditions apparemment disparates que SPECTRUM a corrélées pour créer cette alarme, comme suit :

1. Un domaine de corrélation comportant uniquement les deux routeurs HSRP CPE et les interfaces de routeur PE qui assurent la connexion aux sites
2. Un modèle de règle corrélant la coïncidence d'un événement HSRPGrpStandByState avec un état actif et d'un événement de perte de contact avec le périphérique pour en déduire une condition de perte de connexion principale
3. Un modèle de règle qui définit un événement de liaison incorrecte causé par un événement de perte de connexion principale



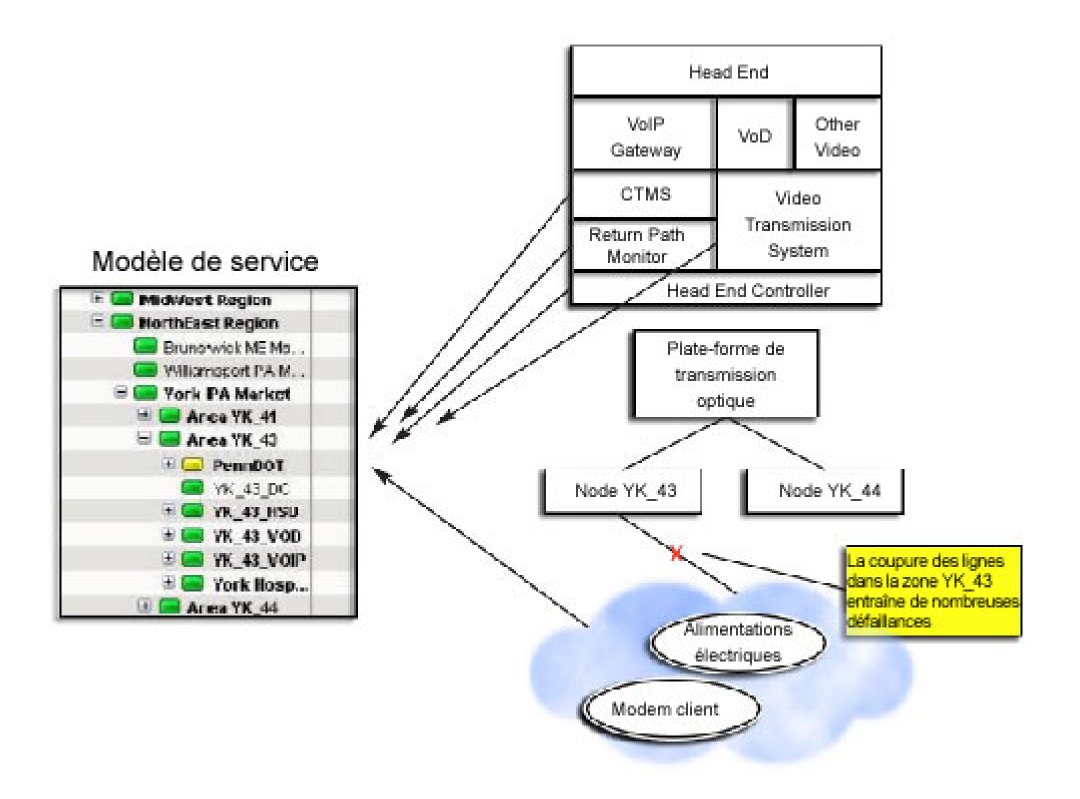
Il applique ces modèles de règles aux domaines de corrélation périmètre.

Sans ces règles, SPECTRUM aurait déclenché une alarme critique sur le périphérique CPE perdu et sur le modèle de port connecté. A l'aide de ces règles, il déclenche une alarme majeure (orange) sur le périphérique CPE indiquant la perte de la connexion principale au client. Les autres conditions s'affichent dans le tableau des symptômes de cette alarme.

Application de la corrélation de conditions à la corrélation de services

En règle générale, les réseaux assurent le transport et la prise en charge de plusieurs services. Par exemple, dans l'industrie du câblage, le service téléphonique (VoIP), l'accès à Internet (données haut débit), la vidéo à la demande et les câbles numériques sont livrés sur le même réseau de données physique. La gestion de ce réseau peut s'avérer très complexe. A l'intérieur du réseau de câblage, l'équipement de transport vidéo, les services d'abonnement vidéo et le CMTS (Cable Model Termination System) fonctionnent conjointement pour placer les données sur le réseau de câblage aux fréquences appropriées. Des kilomètres de câbles, ainsi que des milliers d'amplificateurs et d'alimentations électriques doivent transporter les signaux chez les millions d'abonnés.

Si les lignes réseau sont coupées à un endroit précis, comme indiqué dans le schéma suivant, le système de surveillance du chemin de retour et le contrôleur de tête de réseau signalent les problèmes de chemin de retour et d'alimentation présents à cet endroit. Le CMTS indique le nombre de modems câblés hors ligne pour le noeud correspondant. Le système de transport vidéo renvoie les erreurs de réglage des abonnements vidéo de cette zone. Enfin, le système de gestion perd le contact avec tous les modems clients qu'il gère. Le flux des événements et des messages d'erreur provenant des éléments gérés démontre clairement l'existence de problèmes dans le service ; le défi consiste à traduire toutes ces données en informations utilisables sur la cause première et l'impact sur le service.





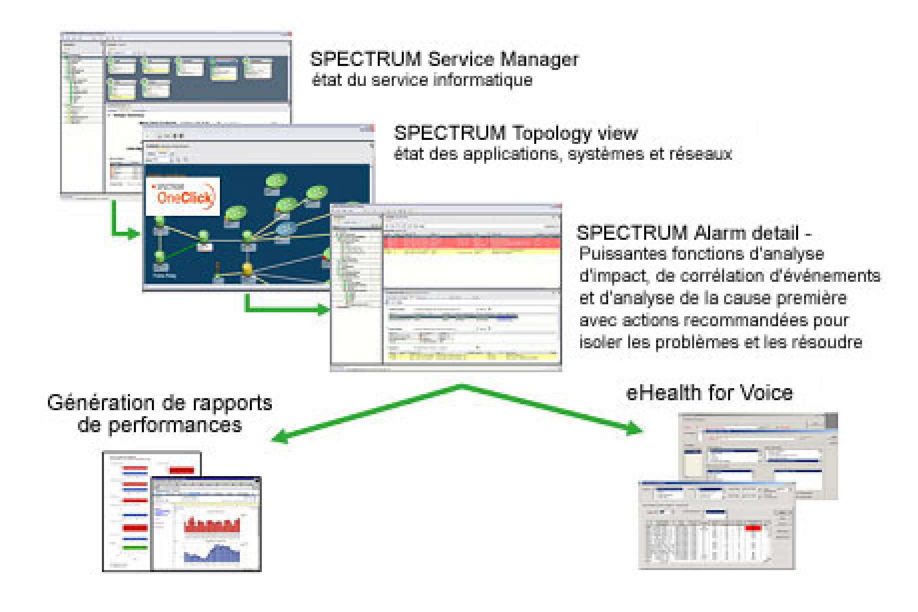
SPECTRUM peut interpréter la profusion d'événements qui en résulte en utilisant la zone de service des événements apparemment disparates en tant que facteur de la corrélation des conditions. Si les services et les zones de service sont modélisés dans SPECTRUM, la corrélation des conditions peut servir à déterminer les services affectés dans chaque zone, ainsi que la ou les causes premières.

Il ne suffit pas de connaître les services affectés ; il est également important d'identifier les éléments qui ne sont *pas* affectés. Il est possible que le service d'abonnement vidéo ne puisse pas fournir le contenu de vidéos à la demande à une zone de service unique alors que tous les autres services fonctionnent normalement. En outre, un problème de chemin de retour dans une zone peut entraîner l'échec des services Internet, VoIP et de vidéo à la demande et la dégradation des câbles numériques, alors que les câbles analogiques continuent à fonctionner normalement. A l'aide des fonctions de SPECTRUM et des vues de votre infrastructure, vous pouvez détecter avec plus de rapidité et de facilité la cause première et vous concentrer sur la résolution du problème.

Exploitation de la solution intégrée

Une fois que SPECTRUM a identifié les problèmes de cause première, le personnel chargé de l'exploitation peut rapidement obtenir des détails sur l'historique des problèmes et des informations de dépannage en analysant de manière plus détaillée les alarmes du navigateur OneClick ainsi que les rapports et les outils *e*Health et *e*Health for Voice. Les opérateurs peuvent, par exemple, cliquer avec le bouton droit de la souris sur une alarme dans OneClick et effectuer l'une des actions suivantes :

- Effectuer un zoom avant sur les rapports Trend pour connaître la variable du problème
- Effectuer un zoom avant sur les rapports At-a-Glance pour obtenir un instantané de plusieurs variables clés de performance de cette ressource
- Effectuer un zoom avant sur la console *e*Health for Voice ou l'interface de génération de rapports Web *e*Health pour afficher davantage de rapports et de détails sur les autocommutateurs privés de voix problématiques et appeler les serveurs de messagerie
- Lancer un navigateur dans l'interface de génération de rapports Web *e*Health pour afficher davantage de rapports et de détails sur les ressources problématiques





(Page laissée intentionnellement vide)



Index





Q

R

S



T





